DISSERTATION

Graphical User Authentication in Smartwatches: A cognitive processing perspective

Eleni Katsi

UNIVERSITY OF CYPRUS

DEPARTMENT OF COMPUTER SCIENCE

May 2019

UNIVERSITY OF CYPRUS
DEPARTMENT OF COMPUTER SCIENCE

Graphical User Authentication in Smartwatches: A cognitive processing perspective

Eleni Katsi

Supervisor
Prof. Andreas Pitsillides

Co-Supervisor
Dr. Marios Belk

The individual thesis submitted for partial fulfillment of the requirements for obtaining the degree of Computer Science, Department of Computer Science in University of Cyprus.

May 2019

ACKNOWLEDGEMENTS

I have had a lot of fun working on this thesis. This has been a hugely enjoyable and fulfilling experience, and I owe much to the people who have supported me throughout it.

First and foremost, I would like to thank Prof. George Samaras who has accepted me to work together on my thesis. Also, many thanks to him for the subject of the thesis he has assigned to me.

I would also like to thank Prof. Andreas Pitsillides, who kindly accepted me to work with him to carry out this thesis when Prof. Samaras deceased in July, 2018.

My research on graphical passwords would not have been possible without the gracious cooperation with Dr. Marios Belk. Special thanks to him for his invaluable support, endless patience and for answering all of my questions. Dr. Marios's enthusiasm and broad knowledge are an inspiration and made working with him a pleasure. His guidance, constructive criticism and encouragement kept me motivated all the time.

Moreover, I would like to extend my thanks to the PhD student Argyris Constantinides, who has been helpful and supportive during the development of my dissertation.

I owe special thanks to a fellow student George Hadjidemetriou who helped me with my experiment.

Furthermore, I must thank all the participants who took part in my evaluation study. This research would have been impossible without their generous contribution of time and effort.

Above all, I am grateful to my parents for their endless love, patience and prayers, for their great support and encouragement. Their experience and advice helped me a lot in my life. My mother and father gave me so much and taught me to appreciate everything.

ABSTRACT

Smartwatches have been seen as the next generation personal devices, after smartphones, due to their use for wide range of applications, e.g., communication, financial applications, social networking and fitness tracking, etc. These applications generate and store a lot of personal and private data which needs to be protected from unauthorized access. Today, authentication is the main measure to guarantee information security and a common authentication method in use, is the PIN-based password. However, their inherent defects led to the development of graphical password as an alternative. Graphical password which uses images as passwords, rather than digits is motivated particularly by the fact that it is generally easier for users to remember and recall images and it is conceivable that graphical password would be able to provide better security than PIN-based password. Furthermore, individuals' cognitive styles may affect the way they create their passwords. The field dependence-independence theory underpins the human cognitive differences in visual perceptiveness and differences in handling contextual information in a holistic or analytic way. This dissertation describes the design and implementation of two smartwatch authentication schemes: PIN-based password and picture password. In addition, a user study was conducted to evaluate the usability and security of the schemes. Analysis of the results has been made and the differences between the two authentication schemes and the human cognitive processing differences (field dependence vs. field independence) were discussed.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

The following table describes the meaning of various abbreviations and acronyms used throughout the thesis.

Term	**Definition**
PIN	Personal Identification Number
JS	JavaScript
CSS	Cascading Style Sheet
SVG	Scalable Vector Graphics
XML	Extensible Markup Language
FD	Field Dependence
FI	Field Independence
GEFT	Group Embedded Figures Test
GUA	Graphical user authentication
JSON	JavaScript Object Notation
POI	Points of Interest
WEP	Wired Equivalent Privacy
WPA	Wi-Fi Protected Access
Wi-Fi	Wireless Fidelity
IP	Internet Protocol
OS	Operating System

CHAPTER 1

1 INTRODUCTION

In recent years, security is supported largely by passwords which are the principle part of the authentication process. A common authentication method is to use PIN-based password which has significant drawbacks. Graphical passwords were proposed as an alternative to overcome the inherent limitations of PIN-based passwords. Recent studies have shown that individuals have different cognitive processing styles and this may affect the way they choose their passwords. The field dependence-independence (FD-I) theory is a cognitive theory interrelated with the ability of an individual to extract visual information in graphical scenes. The individuals, who are classified as FD, tend to follow a more holistic approach to process visual information and have difficulties in identifying details in complex visual scenes. On the other hand, FI individuals tend to follow a more analytic approach to process visual information, pay attention to details and easily separate simple structures from the surrounding visual context.

1.1 MOTIVATION

The main motivation lies with the fact that the human brain is capable of remembering graphical or pictorial objects better than PINs. Also with the advancement of technology, we are now moving forward to using touch based devices such as smartwatches. These on-body wearable devices have become increasingly popular and play significant roles in our daily lives. So with this, the PIN-based password is much more inconvenient in such touch based devices. Therefore, the graphical method would allow the user just to touch the various regions in screen and get authenticated. In addition, convinced that the eye plays an important role in understanding people's intentions and strategies while performing graphical password composition, the field dependence-independence theory suggests that individuals have different habitual

approaches in processing graphical information. Thus, this thesis is based on that FD and FI users might perform differently in various user authentication methods (PIN and graphical).

1.2 OBJECTIVES OF THE THESIS

First aim of the thesis is to develop a prototype of PIN-based password and picture password on smartwatch in order to compare them in terms of usability and security. Also, for each of the two authentication schemes, the goal is to compare the interaction of FDs and FI users. Finally, for FD and FI users the objective is to investigate in which authentication scheme they perform better.

1.3 STRUCTURE OF THE THESIS

The rest of the thesis is organized as follows. Chapter 2 gives an overview of authentication methods and also the usability and security aspects of PIN-based password and picture password are discussed. Chapter 3 discusses the devices and technologies used during the thesis and a reference has also been made to the way the devices communicate with each other. After that, chapter 4 presents the details of the design and implementation of the PIN-based password scheme, the picture password scheme and the server on android phone. Chapter 5 analyses the process of the evaluation study. Chapter 6 presents in detail the results and analysis of the data collected from the evaluation study and chapter 7 concludes the thesis and gives direction for future research.

CHAPTER 2

2 THEORETICAL BACKGROUND

2.1 AUTHENTICATION

As computer technology has become more essential for everybody day by day, providing safe and secure ways to authenticate users to access confidential information or networks on different systems becomes increasingly important too. Verifying the identity of a user, usually referred to as user authentication, is a very important step in almost all kinds of applications. There are currently three main forms of authentication used in computer security systems: token based authentication (something user has), biometric based authentication (something user is), and knowledge based authentication (something user knows). This thesis focuses on both forms of knowledge-based authentication, which are the PIN-based passwords and graphical passwords.

i. Token-based Authentication: In token-based authentication, user is authenticated by possessing and presenting a token to the system [19]. An example of the token can be a key or access card used to open a door. Also, a smart card, i.e., a card with embedded microprocessor chip, is an example of a token used for authentication.

ii. Biometric-based Authentication: Biometric authentication verifies a user based on the user's properties. It uses physiological and/or behavioral characteristics of the human being [25]. Traditional examples of human characteristics that are used as biometrics include fingerprints, facial recognition [20], iris, voice, handwriting.

iii. Knowledge-based Authentication: Knowledge-based Authentication methods are by far the most commonly used authentication schemes today across a wide range of devices and include both PIN based and picture based passwords [26]. In a knowledge-based approach, authentication is based on a secret that is shared between a user and a system [27]. An example of such secret can be a PIN (Personal Identification Number) code.

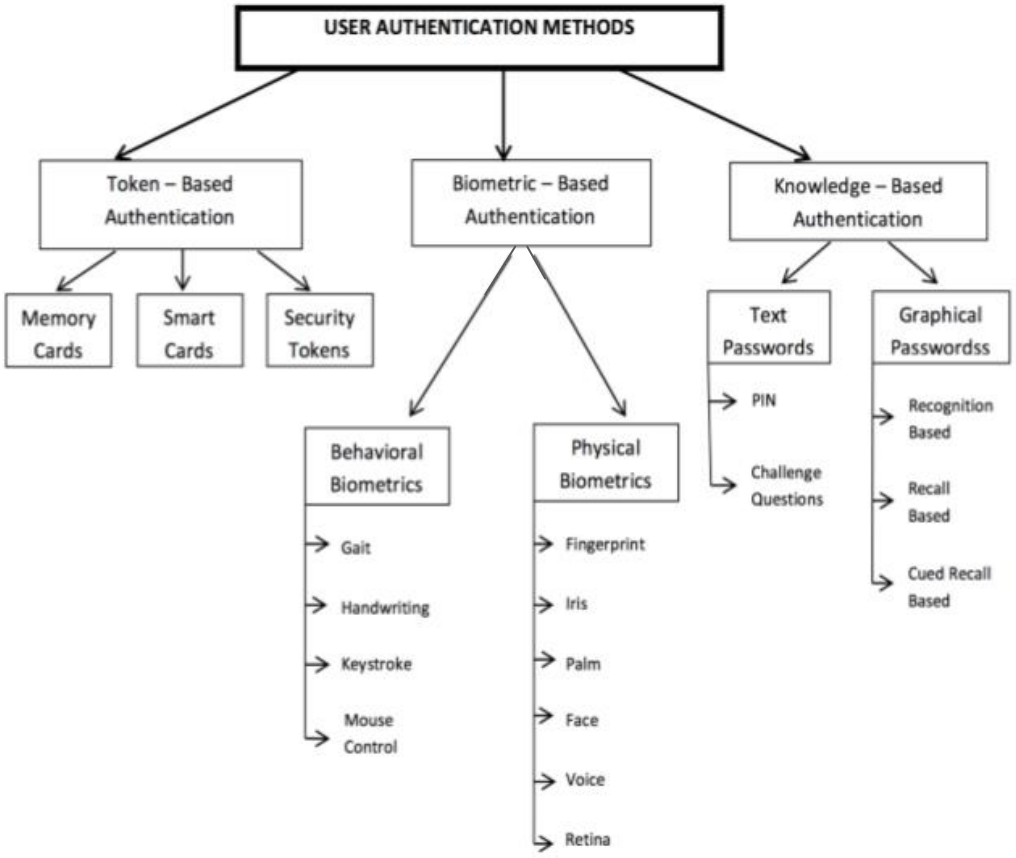


Figure 2.1: User Authentication Methods

2.2 AN OVERVIEW OF PIN-BASED PASSWORD

A Personal Identification Number (PIN) is a kind of text password which is composed of only digits shared between a user and a system that can be used to authenticate the user to the system. A PIN is usually a four-digit number (sometimes six-digit number), thus is consuming less time than other passwords. PINs are used in a variety of security applications where the lack of a full keyboard prevents the use of text passwords such as

electronic door lock codes and smartphone unlock codes. They are commonly used also for telephone systems and automatic teller machines (ATMs) [28].

2.3 AN OVERVIEW OF GRAPHICAL AUTHENTICATION METHODS

Graphical authentication, a term introduced by Blonder [30], has been proposed as a possible alternative to replace the traditional username/password authentication schemes, supported partially by the fact that humans can remember images better than text [32]. In his description of the concept, an image would appear on the screen, and the user would click on a few chosen regions of it. If the correct regions were clicked in, the user would be authenticated [31]. Existing graphical password schemes can be categorized into recall-based, recognition-based and cued-recall [29].

i. Recognition Based Systems: Users can either choose their password images from a collection presented by the system, or the passwords are issued by the system to the users. The users can also provide their own images. During authentication, users must recognize the correct password image among a collection of images. A canonical example is Passfaces [36, 37]. The motivating idea is that humans have a vast memory for images. Also, human beings have an exceptional ability to recognize images that they have previously seen, even if the image has been viewed for a very short period of time.

ii. Recall Based Systems: Users must draw an image either on a grid or canvas during the password creation stage and they have to re-draw that same image during authentication. Some examples are Draw-a-Secret [33] and Pass-Go [34]. However, recall is considered to be the least accurate type of memories because the accuracy would decay after a considerable amount of time, if the password is not used frequently.

iii. Cued-recall Based Systems: Specific points on an image that is either selected by the users or issued by the system, form the password. An archetypal example of such a system is Passpoints [35]. In this kind of systems, the authentication system provides a cue (image) to help the users remember their password (points on the image). This

feature is intended to reduce the memory load on the user and is considered an easier task, compared to unaided recall.

2.4 USABILITY AND SECURITY OF PIN-BASED PASSWORD AND PICTURE PASSWORD

i. PIN-based password: The use of a PIN was introduced as an alternative to text passwords for quicker and more usable solution. When compared to passwords for usability, all of the benefits score the same or better as a result of the technique being so similar, but easier to use. The fact that it only uses numbers and the standard length is four, means that it is much easier for the user to remember it as opposed to passwords. Moreover, it takes less time to enter than the text passwords. In addition, with a PIN the user infrequent makes errors because of the less error-prone numeric keyboard.

However, despite the increases to usability, it scores much lower in security. It scores lower in resilient to shoulder surfing due to being shorter in length and only using numbers so an attacker is able to better identify which keys the user is pressing. It also scores much lower in resilient to smudge attack since finger smudge traces may allow attackers to reconstruct passwords. A PIN also scores lower in resilient to brute-force attack due to the smaller number of possible characters and the fact that the length is usually shorter is reducing the time to break it. Overall, the use of a PIN sacrifices security to make the solution more usable.

ii. Picture password: The picture password was created to utilize the unique touch screen in the hope of being more accurate, reliable, and usable than the error-prone keyboard. It scores higher in usability because the user needs less time to spend in authentication phase and makes fewer mistakes. In addition, the gestures are being fast and accurate compared to typing something into a keyboard. Also, it is easier for a user to remember his password by associating it with an image. Swipe actions require more than the simple tap action of the other techniques, which may be more difficult for someone to perform. Precise swipes require more finger control for the elderly or someone with disabilities.

The security results of picture password are similar to the PIN. Both the resilient to shoulder surfing and the resilient to smudge attack score worse because the swipe persists on the screen and is easy to follow. The main thing that gestures score better on, is resilient to social engineering because for instance to tell a graphical password to others over the phone would be very difficult. Instead of increasing security and making the gesture easier to remember for the user, it makes the gesture easier for the attacker to predict due to "hot spots" on the image that the user is prone to use [5]. These spots narrow the search space for the attacker when they attempt to compromise the device.

2.5 FIELD DEPENDENCE-INDEPENDENCE THEORY

The field dependence-independence (FD-I) theory is a cognitive theory interrelated with the ability of an individual to extract visual information in graphical scenes. The individuals are classified either as FD or FI.

Field - dependent (FD): Concerning the cognitive styles, FD can obtain experiences and perception through integral approach and their perception can be easily affected by the environment. To the autonomy they are dependent on authorities and they are easily affected by other people's criticism. They require extrinsic motivation in order to learn. Regarding to learning methods they have lack the ability to organize learning materials and are more interested in learning things that are related to their own experiences. Also, concerning the emotional control, they have high impulsiveness and lack the ability for emotional regulation [22]. Furthermore, individuals termed as FD are not attentive to detail, cannot abstract an element from its context and tend to handle problems in a holistic way. Accordingly, given that FD individuals view the perceptual field as a whole, they are not efficient and effective in situations where they are required to extract relevant information from a complex whole [4].

Field - independent (FI): Concerning the cognitive styles, FI can obtain experiences and perception through analysis and their perception is not easily affected by the environment. To the autonomy they are based on their own experiences and they are not easily affected by other people's criticism. They have higher intrinsic motivation to learn. Regarding to learning methods they are able to organize learning materials, to

internalize the knowledge and are more interested in learning new things. Also, concerning the emotional control, they have low impulsiveness and better ability for emotional regulation [22]. When confronted with problems, FI individuals are good at extracting things from the context and prefer to handle them in a more analytical way. Given that FI individuals tend to experience items as discrete from their backgrounds and independent to the perceptual field, they are more successful in disembedding and isolating important information from a complex whole [4]. FI individuals are able to discover and distinguish pertinent visual information embedded in an image or environment, and apply a structure to that information [22].

2.6 CONCLUSION

This chapter has presented the background information in order to understand the research presented in this thesis. That is, the current user authentication methods were briefly discussed and reviewed. Also, this chapter has pointed out the usability and security issues of user authentication mainly focusing on PIN-based passwords and picture passwords.

CHAPTER 3

3 APPARATUS AND TECHNOLOGIES FOR CREATING THE APPLICATIONS

3.1 INTRODUCTION

This chapter will discuss the technologies and devices used to develop the various applications. More specifically, the characteristics of each device and the technologies it uses will be mentioned.

3.2 SMARTWATCH

Fitbit Versa is a smartwatch which provides necessary features for everyone. This lightweight smartwatch empowers you to reach health and fitness goals with actionable insights, personalized guidance and on-screen workouts. Also, allows you to track your activity throughout the day, monitor your heartrate, connect to a GPS for real-time pace and distance, access apps and see notifications for calls, calendar events and texts [9]. A new "Today" view shows your current activity stats such as steps or resting heart rate and offers advice on what you can do to increase activity or sleep better [10].

iii. Specifications of Smartwatch [6,7,8]:

Display: 1.34 inches, 300 x 300 pixels

Memory: Saves 7 days of detailed motion data – minute by minute

Battery: Lithium-polymer, 145mAh, 4+ Days

Wi-Fi: Wi-Fi 802.11 b/g/n

Radio transceiver: Bluetooth 4.0

Internal Memory: 4GB (2.5GB available, 300+ Songs)

Operating System: Fitbit OS

Water Resistance: Up to 50 meters

Sensors: 3-axis accelerometer, 3-axis gyroscope, Optical heart rate monitor, Altimeter, Ambient light sensor, SpO2 sensor

Other Features: 15+ Exercise Modes, Activity tracking and step counting, Sleep tracking, Coaching functions, 24/7 heart rate tracking, Music with Deezer integration, Fitbit Pay supported, Smartphone notifications, Female health tracking.

Figure 3.1: Fitbit Versa

iv. Fitbit Studio: Fitbit Studio is a tool (an online IDE) to create Fitbit apps and clock faces from anywhere for Fitbit OS devices, such as Fitbit Ionic, Fitbit Versa, and Fitbit Versa Lite. It's using JavaScript, CSS, and SVG which make developers have a fast, easy way to build apps and clock faces for Fitbit OS.

JavaScript (JS): JavaScript is a lightweight interpreted or just-in-time compiled programming language with first-class functions. It is most well-known as the scripting language for web pages. JavaScript is a prototype-based, multi-paradigm, dynamic language, supporting object-oriented, imperative, and declarative (e.g. functional programming) styles [11]. The application logic of Fitbit apps and clock faces, is written in JavaScript (.js) files, and can interact with the user interface using document object events and functions [12].

Cascading Style Sheets (CSS): Cascading Style Sheets is a style sheet language used for describing the presentation of a document written in a markup language. CSS is designed to enable the separation of presentation and content [13]. Stylesheets written in

CSS (.css) files can be used to control the appearance (color, size, font and position) of the elements within the Fitbit application user interface [14].

Scalable Vector Graphics (SVG): Scalable Vector Graphics (SVG) is an XML-based vector image format for two-dimensional graphics with support for interactivity and animation [15]. In addition to the standard SVG elements provided, in Fitbit Studio there are a number of predefined SVG components to simplify the development process, and to allow developers to create rich user interfaces [16].

3.3 ANDROID SMARTPHONE

The Samsung Galaxy Note II GT-N7100 is an Android smartphone. This phone device has plenty of processing power for Web browsing, video streaming and working within multiple windows. Features like one handed operation functions, shortcuts on the notification menu, screen rotation and a dedicated number row above the keyboard make the phone convenient and simple to use. This phone also supports voice dictation in addition to photo and video inserts. The touchscreen is responsive to touch but has a feature that makes it sensitive enough to the S Pen so that users do not have to worry about accidentally hitting a back button or erasing written notes [18].

i. Specifications of Smartphone [17]:

Display: 5.5 inches, 720 x 1280 pixels
Processor: 1.6GHz quad-core
RAM: 2GB
Operating System: Android 4.1
Storage: 16GB
Battery Capacity: 3100mAh

Figure 3.2: Samsung Galaxy Note II GT-N7100

ii. Android Studio: The Android Studio is an open source and Linux-based operating system and is designed specifically for Android development. Every project contains java programming language and XML layouts.

3.4 COMMUNICATION SETUP BETWEEN SMARTWATCH AND SMARTPHONE

i. Store data on the server: As users interact with smartwatch, lot of data about their moves are retrieved. These data should be sent to the server and stored there for later analysis. However, because they cannot be sent directly from the smartwatch to the server, there is an intermediate stage, the companion. The companion is actually the Fitbit application of the phone. That is, the data from smartwatch is sent to the companion of the phone and from there to the android application which is the server. Thus, the server stores the data in a JSON file.

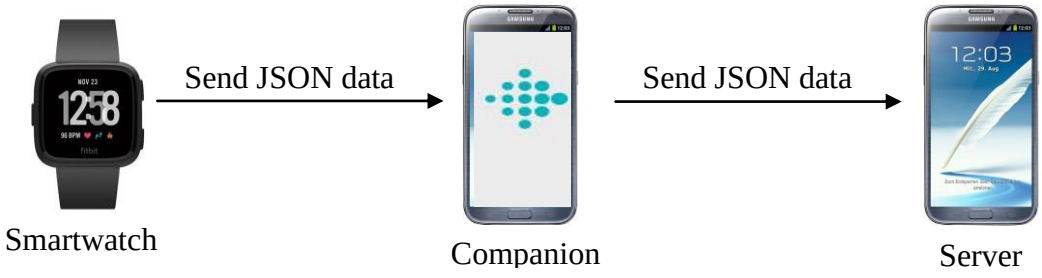


Figure 3.3: Communication architecture between devices to store data on the server

ii. Get data from the server: As users interact with smartwatch, data stored on the server must be sent several times to smartwatch so that they can continue to interact. These data, however, because they cannot be sent directly from the server to the smartwatch, an intermediate stage must exist which is the companion. The companion is actually the Fitbit application of the mobile. That is, smartwatch sends a request for specific data to the companion, and the companion sends the request to the android application that is the server. The server receives the request and sends the appropriate data back to the companion. So the data from the companion are sent back to the smartwatch and then the user interaction with the smartwatch can continue.

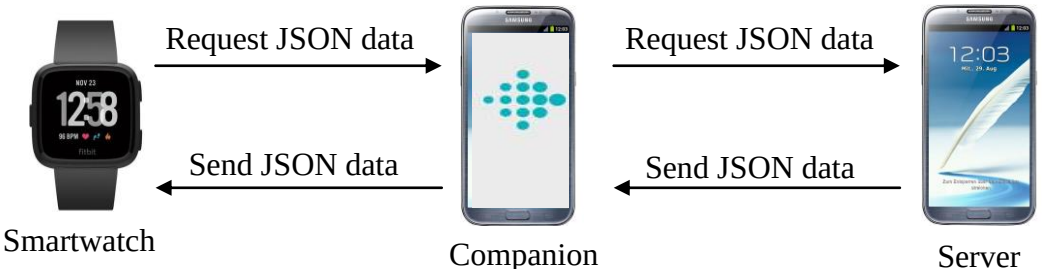


Figure 3.4: Communication architecture between devices to get data from the server

3.5 CONCLUSION

This chapter has analyzed the devices and technologies used during the thesis. Reference has also been made to the way the devices communicate with each other in order to exchange various data.

CHAPTER 4

4 DESIGN AND IMPLEMENTATION OF USER AUTHENTICATION SCHEMES

4.1 INTRODUCTION

User authentication is one of the most important parts of the security of information systems. A common approach for authenticating users is PIN passwords. As mentioned before, users generally choose weak passwords to remember them easily. This increases the possibility of the passwords to be hacked by attackers. When users are requested to create long and complex passwords, they resort to copy strategies such as writing passwords down or reusing them. Therefore, PIN passwords suffer from various drawbacks and vulnerabilities to attacks. On the other hand, graphical passwords are considered as a good replacement for PIN passwords. The fact that humans can recognize and remember images easily over PIN can be a solution to the memorability problem. However, they are more vulnerable to shoulder surfing attacks. In order to compare the usability and security aspects between PIN-based and graphical-based passwords, I have designed and implemented these two approaches for authenticating users. Therefore, this chapter will focus and go into detail about the design and implementation of the PIN-based password scheme and picture password scheme.

4.2 PIN-BASED PASSWORD SCHEME

The PIN-based password scheme is an authentication approach, in which the user would have to select six digits and remember them, as his or her password.

For each of the six digits of the password, the user can select one digit from 0 to 9. Also, the user is allowed to select the same digit more than once. Thus, this PIN-based password scheme produces more or less 1,000,000 different passwords (user can select one of the 10 digits each time => 10x10x10x10x10x10 = 1,000,000).

This PIN-based password scheme was implemented in smartwatch.

4.2.1 Registration Phase

In the registration phase, user enters a user ID that has not already been taken by another user and then chooses his/her password by clicking several digits that are displayed. The password that the user selected is stored in a JSON file along with the entered user ID and other parameters which will be explained later. Screenshots of various screens are shown later.

More specifically, the initial screen consists of two labels: "Admin" and "PIN-based Password" (see Figure 4.1). The "Admin" label redirects the user to "Admin" screen and the "PIN-based Password" label redirects to the "PIN-based Password" screen. The "Admin" screen consists of two buttons and one label (see Figure 4.2). The buttons are: "New User" and "Switch User". Both buttons redirects the user to another screen. The two screens to which users were redirected by these buttons are identical in appearance but each screen performs a different function. The "New User" screen, inserts a new user to the file. The "Switch User" screen adds another record to a user that is already in the file. On these screens the user has to put his/her user ID (see Figure 4.3). They are consisting of twelve buttons and two labels. The first label has the text "UserID:" and the second label shows the user ID that the user selects. Ten of twelve buttons are the digits from 0 to 9 which the user has to press in order to insert his/her user ID. The button on the bottom right is the "Backspace" and the button on the bottom left is the "Done". When the "Backspace" button is pressed, the last digit of the user ID is deleted

and when the "Done" button is pressed, means that the user has put his/her user ID and is redirected to the "Admin" screen. The label on the bottom of the "Admin" screen shows the selected user ID (see Figure 4.4). In the "Admin" screen, when the user press the back button of smartwatch, is redirected to the initial screen. Pressing the "PIN-based Password" label, the user redirects to the "PIN-based Password" screen which is consisted of two labels: "Create" and "Login" (see Figure 4.5). Pressing the label "Create" the user is redirected to the "Create" screen and is asked to create his/her PIN-based password (see Figure 4.6). The "Create" screen is consisted of one label and eleven buttons. Ten of eleven buttons are the digits from 0 to 9 which the user has to press in order to insert his/her password. The button on the bottom right is the "Backspace" and when it is pressed, the last digit of the password is deleted. The label on the top of the screen informs the user to enter new password. This label disappears when a button with a digit is pressed and six dots (one for each digit of the password) appear. At the beginning, the dots are transparent and if for instance the user enters the first four digits of his/her password, then the first four dots are not transparent anymore and the rest two dots remain transparent (see Figure 4.7). When the user enters six digits as his/her password, is redirected to another screen in order to confirm his/her password (see Figure 4.8). The "Confirm" screen is the same with the "Create" screen but the label on the top informs the user to re-enter the password. As in "Create" screen the label disappears when a button with a digit is pressed and six dots (one for each digit of the password) appear (see Figure 4.9). Also, in "Confirm" screen on the bottom left there is a "Start Over" button that did not exist in "Create" screen. Pressing this button means that the user wants to enter again a new password. So, he/she is redirected to the "Create" screen and the password is initialized. If the registration is unsuccessful he is redirected to the "Confirm" screen again and the user can try again his PIN password. When the user enters a new password and confirms it successfully, then he/she has created his/her PIN-based password and he/she is redirected to the "PIN-based Password" screen. Then he/she has to go to the "Login" screen which will be explained in the next section.

The registration phase of the scheme is illustrated below step by step with an example user ID.

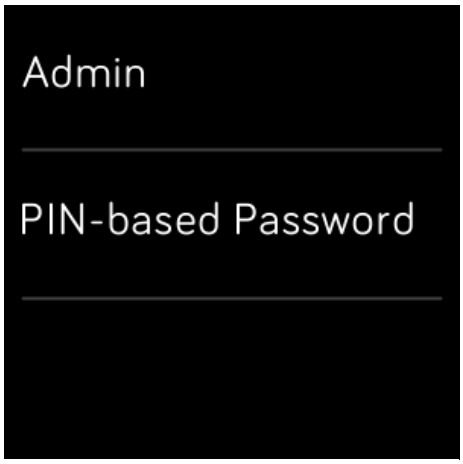


Figure 4.1: Initial screen for PIN-based password

Figure 4.2: Admin screen for PIN-based password

Figure 4.3: New User screen for PIN-based password

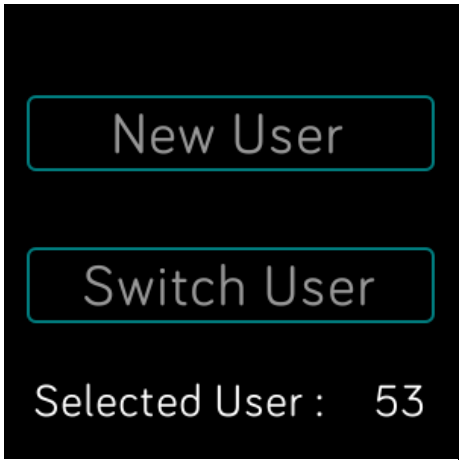


Figure 4.4: Admin screen after the selection of user ID for PIN-based password

Figure 4.5: PIN-based password screen

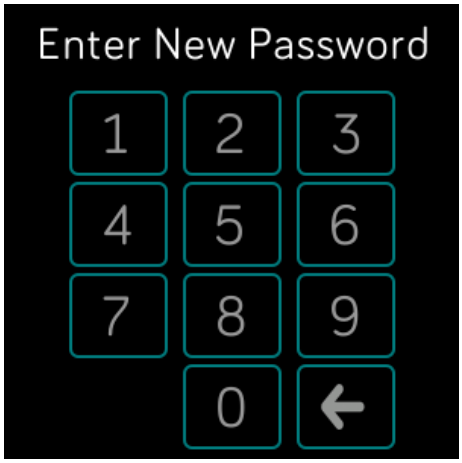


Figure 4.6: Create screen for PIN-based password

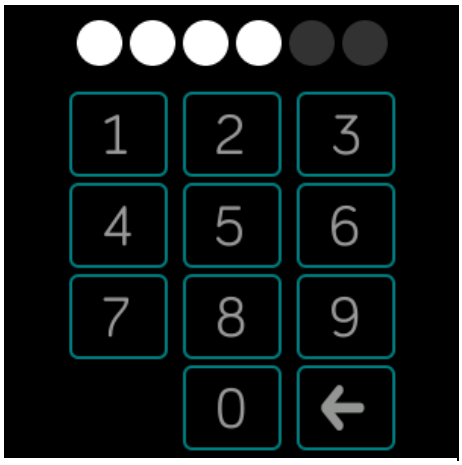


Figure 4.7: Create screen after entering the first four digits for PIN-based password

Figure 4.8: Confirm screen for PIN-based password

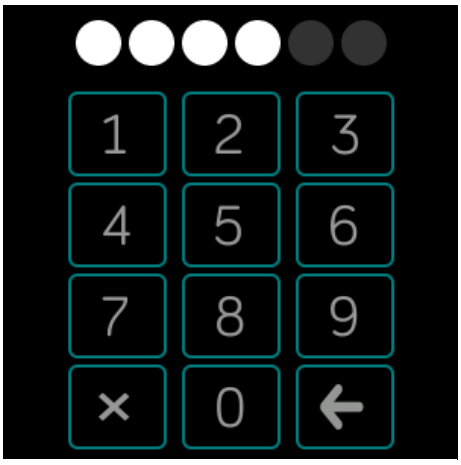


Figure 4.9: Confirm screen after entering the first four digits for PIN-based password

4.2.2 Authentication Phase

In the authentication phase user enters in the same sequence the digits he had selected during registration phase. The entered PIN password is matched against the one stored in the JSON file. If a match is found, the user is successfully authenticated, otherwise the user will not have an access and he has to try again. Screenshots of various screens are shown later.

More specifically, when the user has created his PIN-based password successfully and he has redirected to the "PIN-based Password" screen, he can press the "Login" label and go to the "Login" screen. The "Login" screen is similar to the "Create" screen. When the user is redirected to the "Login" screen is asked to enter his PIN password (see Figure 4.10). The "Login" screen is consisted of one label and eleven buttons. Ten of eleven buttons are the digits from 0 to 9 which the user has to press in order to enter his password. The button on the bottom right is the "Backspace" and when it is pressed, the last digit of the password is deleted. The label on the top of the screen informs the user to enter the password which has been created to the registration phase before. This label disappears when a button with a digit is pressed. Six dots (one for each digit of the password) appear at the same time. At the beginning, the dots are transparent and if for example the user enters the first four digits of his password, then the first four dots are not transparent anymore and the rest two dots remain transparent (see Figure 4.11). When the user enters his PIN password, it checks whether the entered PIN password is the same with the PIN password which is stored in the JSON file. If the password is incorrect, the user is redirected to another screen in order to re-enter his password and try again (see Figure 4.12). The "re-enter password" screen is similar to the "Login" screen, but now the label on the top of the screen informs the user to re-enter the PIN password. Otherwise, if the password is correct then the user is logged in successfully and is redirected to a screen which asks him if he wants to see his heart rate (see Figure 4.13). If he clicks to the button "Yes" then he is redirected to a screen which shows his heart rate (see Figure 4.14), otherwise if he clicks to the button "No", he is redirected to the initial screen.

On most of the screens, the user can navigate to the previous screen by pressing the back button of smartwatch (see Figure 4.15).

The authentication phase of the scheme is illustrated below step by step.

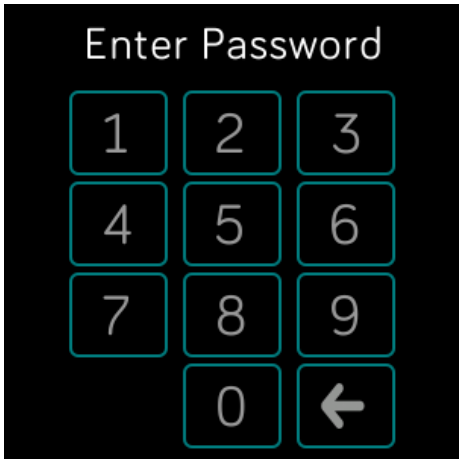


Figure 4.10: Login screen for PIN-based password

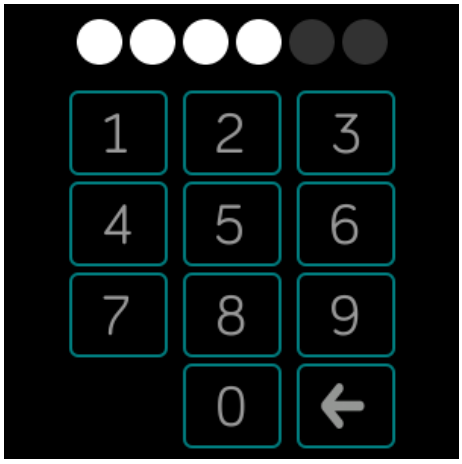


Figure 4.11: Login screen after entering the first four digits for PIN-based password

Figure 4.12: Re-enter password screen for PIN-based password

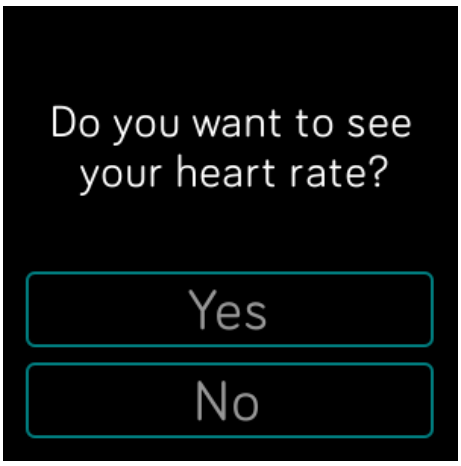


Figure 4.13: Heart rate screen for PIN-based password

Figure 4.14: User's heart rate screen for PIN-based password

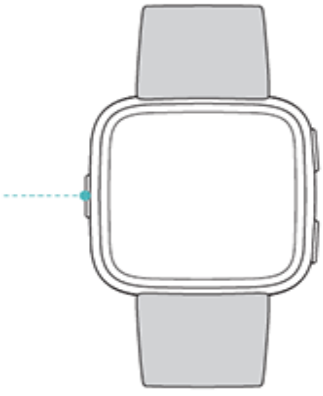


Figure 4.15: The back button of the smartwatch

4.2.3 File Setup

As mentioned earlier a JSON file is used for storing the data of the users. This section will describe the structure of the JSON file. For PIN-based password scheme there are two tables created: "pinCreate" and "pinLogin". The "pinCreate" table is the table storing the user data of the registration phase of the PIN-based password scheme and the "pinLogin" table has the main purpose to keep track of the user data of the authentication phase of the PIN-based password scheme. The attributes that the "pinCreate" table has are: user ID, session ID, time to create the PIN password and time to confirm the PIN password, retries made in registration phase, if the user has successfully created his PIN password, if it is the current record, the PIN password that the user has entered and the date that he has created his PIN password. The attributes that the "pinLogin" table has are the user ID, session ID, time to login, the trials made in authentication phase, if the user successfully logged in, if is the current record and the date that he logged in. An example of the tables can be seen below, with two users.

User ID	SessionID	TimeCreate	TimeConfirm	Retries	Successful	IsCurrent	PIN	DateCompleted
1	1	2098	3109	1	1	1	911997	22/2/2019 11:06
2	1	4864	4591	0	1	1	431995	22/2/2019 13:11

Table 4.1: pinCreate table structure

User ID	SessionID	TimeLogin	Trials	Successful	IsCurrent	DateCompleted
1	1	3345	1	1	1	22/2/2019 11:07
2	1	5120	2	1	1	22/2/2019 13:12

Table 4.2: pinLogin table structure

4.3 PICTURE PASSWORD SCHEME

The picture password scheme is based on the recall authentication scheme, in which the user would have to click in a certain set of places of the picture and remember the sequence of the clicked points to be authenticated. The scheme is made simple so as to avoid much stress to the user while registration and authentication phase.

This scheme uses one image of 300x300px. The user has to click five points as his or her password. The image is divided into a 4x4 grid, which means that each segment is 75x75px. Although the image is divided into a grid, in the authentication phase, there is a small chance that a user will not click exactly on the same segment of the image that he clicked in the registration phase. This can happen when, in the registration phase, the user clicks a pixel which is near one of the edges of the segment. So during the authentication phase it's easy not to click the same segment but in a neighbouring one. For this reason there is a tolerance with which a slight deviation from the original point is considered as the correct point. A 30px radius around the original point is chosen to be considered as the threshold radius. This means that, in authentication phase, a user have to click within a 75x75px area of the original segment or 30px next to the original segment in order to be authenticated.

So, for each of the five clicks of the password, the user can click on one of the 16 segments. Also, the user is allowed to click on the same segment more than once. Thus, this picture password scheme produces more or less 1,048,576 different passwords (user can click on one of the 16 segments for each of the five clicks => 16x16x16x16x16 = 1,048,576).

This picture password scheme was implemented in smartwatch.

4.3.1 Registration Phase

In the registration phase, user enters a user ID that has not already been taken by another user and then chooses his password by clicking several interest points on the displayed image. The coordinates of the clicked points are collected and stored in a

JSON file along with the entered user ID and other parameters which will be explained later. Screenshots of various screens are shown later.

More specifically, the initial screen consists of two labels: "Admin" and "Picture Password" (see Figure 4.16). The "Admin" label redirects the user to "Admin" screen and the "Picture Password" label redirects to the "Picture Password" screen. The "Admin" screen consists of two buttons and one label (see Figure 4.17). The buttons are: "New User" and "Switch User". Both buttons redirects the user to another screen. The two screens to which users were redirected by these buttons are identical in appearance but each screen performs a different function. The "New User" screen, inserts a new user to the file. The "Switch User" screen adds another record to a user that is already in the file. On these screens the user has to put his user ID (see Figure 4.18). They are consisted of twelve buttons and two labels. The first label has the text "UserID:" and the second label shows the user ID that the user selects. Ten of twelve buttons are the digits from 0 to 9 which the user has to press in order to insert his user ID. The button on the bottom right is the "Backspace" and the button on the bottom left is the "Done". When the "Backspace" button is pressed, the last digit of the user ID is deleted and when the "Done" button is pressed, means that the user has put his user ID and is redirected to the "Admin" screen. The label on the bottom of the "Admin" screen shows the selected user ID (see Figure 4.19). In the "Admin" screen, when the user presses the back button of smartwatch, is redirected to the initial screen. Pressing the "Picture Password" label, the user redirects to the "Picture Password" screen which is consisted of two labels: "Create" and "Login" (see Figure 4.20). Pressing the label "Create" the user is redirected to the "Create" screen and is asked to create his picture password. The "Create" screen is consisted of one image (see Figure 4.21). So, the user has to click on any points on the image. After a click of the user a number appears on the top left of the image, which informs the user how many clicks he has done. If for instance the user clicks four times, then the numbers 1, 2, 3 and 4 will appear (see Figure 4.22). When the user clicks five times on the image, is redirected to another screen which informs him to confirm his gestures (see Figure 4.23). By clicking to the "Next" button the user is redirected to the "Confirm" screen which is the same with the "Create" screen. As in "Create" screen after a click of the user a number appears on the top left of the image, which informs the user how many clicks he has done. If the

registration is unsuccessful a failure message is shown on a new page with two buttons: "Retry" and "Start Over" (see Figure 4.24). Pressing the button "Retry", the image is displayed again and the user can try again his picture password. Pressing the "Start Over" button means that the user wants to enter again a new picture password. So, he is redirected to the "Create" screen and the password is initialized. If the registration is successful, then a success message is shown on a new page with a button "Finish" (see Figure 4.25). Pressing the "Finish" button the user data and the coordinates of the clicked points are stored into the JSON file and the user is redirected to the "Picture Password" screen. Then he has to go to the "Login" screen which will be explained in the next section.

The registration phase of the scheme is illustrated below step by step with an example user ID.

Figure 4.16: Initial screen for picture password

Figure 4.17: Admin screen for picture password

Figure 4.18: New User screen for picture password

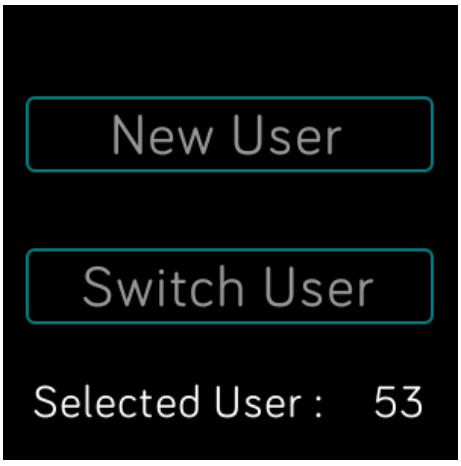


Figure 4.19: Admin screen after the selection of user ID for picture password

Figure 4.20: Picture password screen

Figure 4.21: Create screen for picture password

Figure 4.22: Create screen after clicking four times for picture password

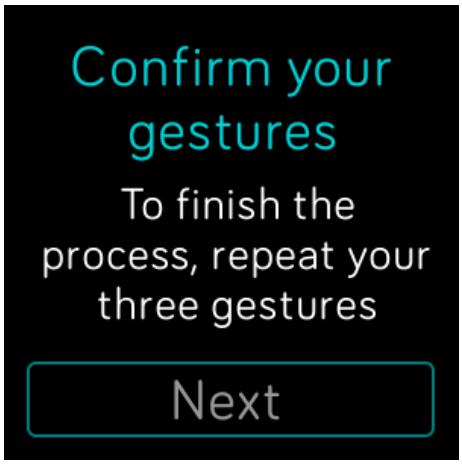


Figure 4.23: Screen that informs about the confirmation for picture password

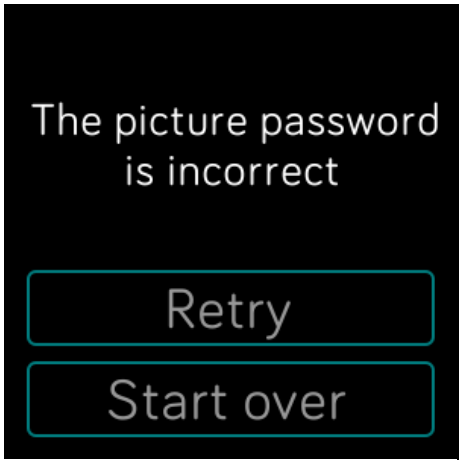


Figure 4.24: Failure screen for picture password

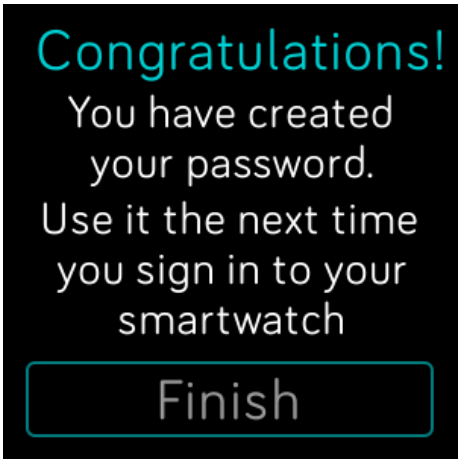


Figure 4.25: Congratulations screen for picture password

4.3.2 Authentication Phase

In the authentication phase the user enters his picture password in the same sequence as he had done during registration phase. The entered picture password is matched against the one stored in the JSON file. If a match is found, the user is successfully authenticated, otherwise the user will not have an access and he has to try again. Screenshots of various screens are shown later.

More specifically, when the user has created his picture password successfully and he has redirected to the "Picture Password" screen, he can press the "Login" label and go to the "Login" screen. The "Login" screen is similar to the "Create" screen. When the user is redirected to the "Login" screen, he is asked to enter his picture password. The "Login" screen is consisted of one image (see Figure 4.26). After a click of the user a number appears on the top left of the image, which informs the user how many clicks he has done. When the user clicks five times on the image, it checks whether the clicked points are within the tolerance region of the original points stored in the JSON file. If the picture password is incorrect, the user is redirected to another screen which informs him that the picture password is incorrect (see Figure 4.27). Pressing retry the user is redirected to the "Login" screen in order to enter again his password. Otherwise, if all the points are correct and in the same sequence then the user is logged in successfully and is redirected to a screen which asks him if he wants to see his heart rate (see Figure

4.28). If he clicks to the button "Yes" then, he is redirected to a screen which shows his heart rate (see Figure 4.29), otherwise if he clicks to the button "No", he is redirected to the initial screen.

On most of the screens, the user can navigate to the previous screen by pressing the back button of smartwatch.

The authentication phase of the scheme is illustrated below step by step.

Figure 4.26: Login screen for picture password

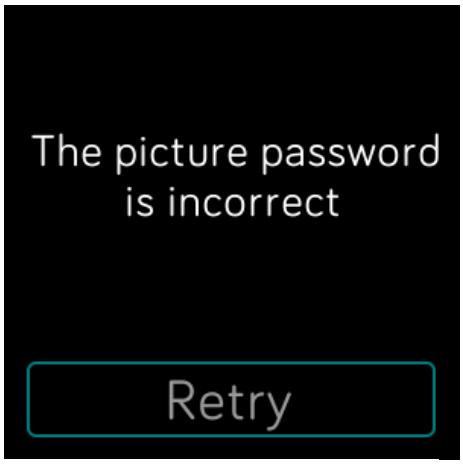


Figure 4.27: Failure to login screen for picture password

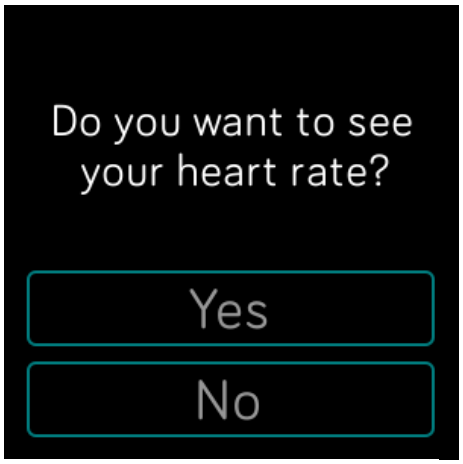


Figure 4.28: Heart rate screen for picture password

Figure 4.29: User's heart rate screen for picture password

4.3.3 File Setup

As mentioned earlier a JSON file is used for storing the data of the users. For picture password scheme there are two tables created: "pictureCreate" and "pictureLogin". The "pictureCreate" table is the table storing the user data of the registration phase of the picture password scheme and the "pictureLogin" table has the main purpose to keep track of the user data of the authentication phase of the picture password scheme. The attributes that the "pictureCreate" table has are: user ID, session ID, time for gesture 1, time for gesture 2, time for gesture 3, time for gesture 4, time for gesture 5 and time to confirm. The table also has: retries made in registration phase, if the user has successfully created his picture password, if it is the current record, the segment of the gesture 1, the segment of the gesture 2, the segment of the gesture 3, the segment of the gesture 4, the segment of the gesture 5, the coordinates (x, y) of gesture 1, the coordinates (x, y) of gesture 2, the coordinates (x, y) of gesture 3, the coordinates (x, y) of gesture 4, the coordinates (x, y) of gesture 5 and the date that he has created his picture password. The attributes that the "pictureLogin" table has are: the user ID, session ID, time for gesture 1, time for gesture 2,time for gesture 3, time for gesture 4, time for gesture 5, the trials made in authentication phase, if the user has successfully logged in, if it is the current record and the date that he logged in. An example of the tables can be seen below, with two users.

User ID	SessionID	TimeGest1	TimeGest2	TimeGest3	TimeGest4	TimeGest5	TimeConfirm	Retries
1	1	2476	815	744	750	586	2866	0
2	1	1289	1342	3694	1763	1309	4362	0

Successful	IsCurrent	Segm1	Segm2	Segm3	Segm4	Segm5	Gest1x1	Gest1y1
1	1	5	7	8	16	14	56	95
1	1	7	16	15	5	8	168	86

Gest2x1	Gest2y1	Gest3x1	Gest3y1	Gest4x1	Gest4y1	Gest5x1	Gest5y1	DateCompleted
172	82	299	84	280	244	148	241	22/2/2019 11:04
256	254	151	228	64	96	289	87	22/2/2019 13:07

Table 4.3: pictureCreate table structure

User ID	Session ID	Time Gest1	Time Gest2	Time Gest3	Time Gest4	Time Gest5	Trial	Successful	IsCurrent	DateCompleted
1	1	1440	460	493	480	335	1	1	1	22/2/2019 11:05
2	1	1057	811	863	738	817	1	1	1	22/2/2019 13:08

Table 4.4: pictureLogin table structure

4.4 TRAINING APP FOR PICTURE PASSWORD SCHEME

This app has been developed to help users familiarize themselves with the picture password scheme. This is because users are familiar with the PIN-based password rather than the picture password. So before users create their picture password they are trained first to become more familiar with this kind of password. The training app works just like the picture password scheme but with two small differences. The first is that the image in which the user clicks on is different form the picture password scheme and also the coordinates of the points that the user has clicked, are not stored in a file but in temporary variables.

More specifically, the first three screens are informative to the user (see Figure 4.30, Figure 4.31 and Figure 4.32). Then the image appears and the user has to click five times on it. After that the user is redirected to a screen that informs him to confirm his gestures (see Figure 4.35). Pressing the button "Next" is redirected to the "Confirm" screen. If he has created his picture password successfully then the user is redirected to a screen with a congratulations message (see Figure 4.37), otherwise he is redirected to a screen which informs him about the wrong picture password that he entered (see Figure 4.36). He can try again to confirm his password pressing the "Retry" button or create his password from the beginning pressing the "Start Over" button.

On most of the screens, the user can navigate to the previous screen by pressing the back button of smartwatch.

The training process is illustrated below step by step.

Figure 4.30: First informative screen for training app

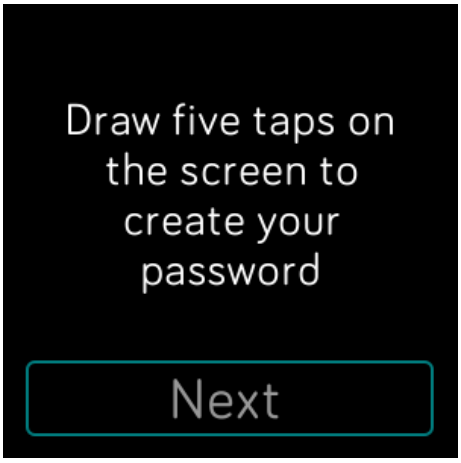


Figure 4.31: Second informative screen for training app

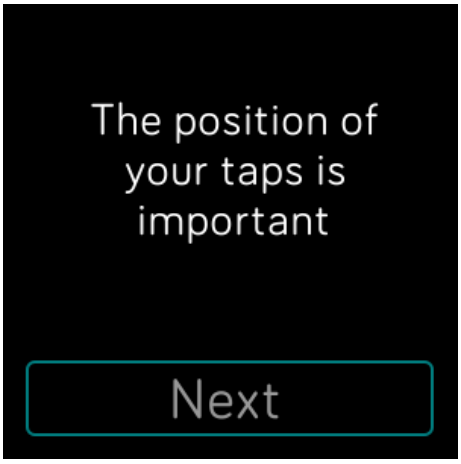


Figure 4.32: Third informative screen for training app

Figure 4.33: Create screen after the first click for training app

Figure 4.34: Create screen after the second click for training app

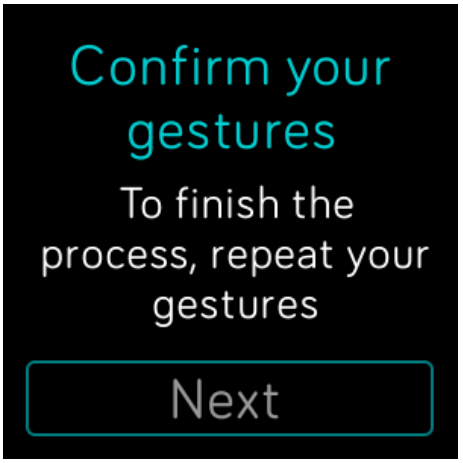


Figure 4.35: Screen that informs about the confirmation for training app

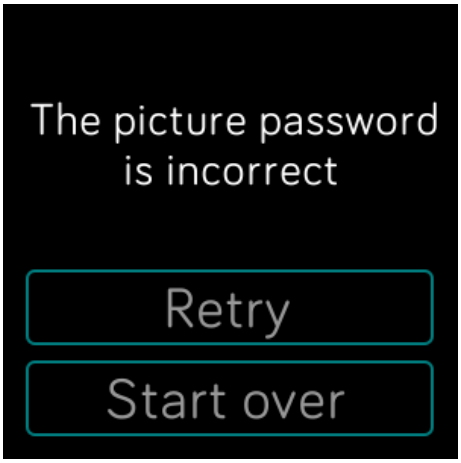


Figure 4.36: Failure screen for training app

Figure 4.37: Congratulations screen for training app

4.5 ANDROID APP

Server:

The user data received from the smartwatch is stored in a JSON file on the phone. In order to do this, a web server on android is used. That is, the library NanoHttpd [39] is used. The NanoHTTPD is a lightweight HTTP server designed for embedding in other applications. I've extended the server to achieve the wanted functionality. That is, I have written code in order to get the data sent to the server by the smartwatch and store them in a JSON file.

The android app is simple and has two buttons: START and STOP to start and stop the server respectively (see Figure 4.38). Also, once the START button is pressed, the IP address and the port on which the server is running appear on the screen (see Figure 4.39).

The server is illustrated below.

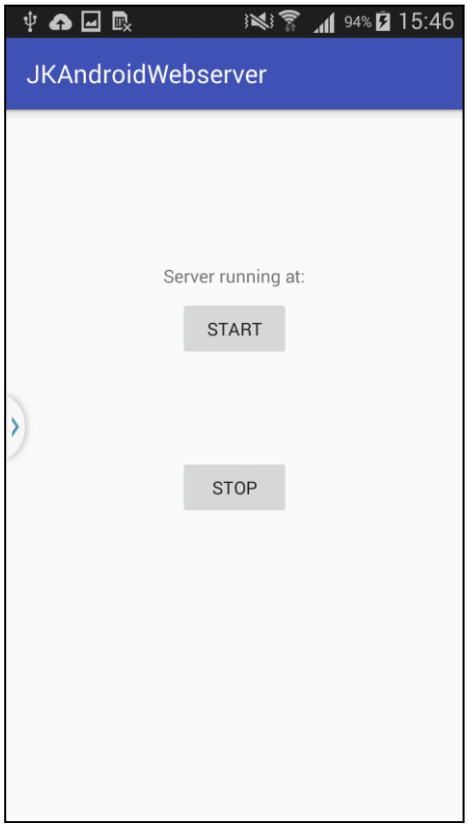


Figure 4.38: Server on android app

Figure 4.39: Android app after pressing the START button

4.6 CONCLUSION

This chapter presented the details of the design and implementation of the PIN-based password scheme, the picture password scheme and the server on android phone. All these applications needed to be developed in order to run the evaluation study, which will be explained in the next chapter.

CHAPTER 5

5 EVALUATION STUDY

5.1 MOTIVATION OF THE EVALUATION STUDY

This evaluation study is primarily motivated by the fact that the human mind variates in cognitive processing styles and abilities among individuals. Among the various cognitive styles, field independence (FI) and field dependence (FD) are frequently studied and used in research. Field dependence-independence refers to the way individuals gain, store, process, and use information [2]. Furthermore, FD and FI users might perform differently in various user authentication types, for instance PIN and graphical, since the way the task is performed in each case is different. Consequently, the goals of this evaluation study are to investigate the relation between human cognitive factors (FD/FI) and user authentication schemes (PIN/graphical) towards usability and security aspects.

5.2 STUDY INSTRUMENTS

In this study, the following study instruments were used: PIN-based Password Scheme, Graphical User Authentication (GUA) scheme, GEFT test and interaction devices.

i. PIN-based Password Scheme: The PIN-based password scheme is an authentication approach, in which the user has to select six digits and remember them, as his/her password.

ii. Graphical User Authentication (GUA) scheme: A recall-based graphical authentication scheme was designed and developed in which the user has to click five times on the picture and remembers the sequence of the clicked points to be authenticated.

iii. GEFT test: Users' field dependence-independence was measured through the Group Embedded Figures Test (GEFT) by Oltman et al. (1971) [24] which is a widely validated paper-and-pencil test [21, 22]. The test measures the user's ability to find common geometric shapes in a larger design. The GEFT consists of 25 items which are divided in three sections. The first section consists of 7 items which are only used for practice purposes and the individual has two minutes to solve them. The second and the third sections consist of 9 items each and are used for assessment. The individual has five minutes to complete each of these sections. In each item, a simple geometric figure is hidden within a complex pattern, and participants are required to identify the simple figure quickly by drawing it with a pencil over the complex figure without being distracted by irrelevant lines. The score is calculated by summing the correct answers in the last two sections. Therefore, the score ranges between 0 and 18 and the individuals are classified as either FD or FI with the use of a cut-off score [22]. Participants that solve 11 items and less are classified as FD and participants that solve 12 items and above are classified as FI.

iv. Interaction devices: Smartwatch (Fitbit Versa), Smartphone (Galaxy Note II).

5.3 PARTICIPANTS

A total of 50 individuals (35 females and 15 males) participated in this study. The participant pool included graduate and undergraduate students from our university and other universities and some people who work. All participated voluntarily and could stop any time they wished. 5 participants had owned or used smartwatches before this study. All participants expressed that they would be concerned if someone gains access to their smartphone or smartwatch and believe that it is important to have a locking method to keep others away. Based on the users' GEFT scores, 18 participants were classified as FD and 32 participants as FI (GEFT score: M = 12.34, SD = 4.26, min = 2,

max = 18). Half of the participants who were classified as FD started with the PIN-based password scheme while the other half of them started with the picture password scheme. The same happened with the participants who were classified as FI. All data collected during this study was used in an anonymized way (i.e. there was no link between the collected data and an individual user).

5.4 PROCEDURE AND STEPS

The study was comprised of three phases.

Phase A: The experiment was completely individual. After welcoming the participant, was given a brief information about the purpose and procedure of the experiment as well as what he would do during the study. He was informed about the data that would be collected during the study and that it would be stored anonymously and used only for research purposes. After clearing up any questions the participant had, he asked to read, accept and sign the consent form if he decided to participate. Once the participant had accepted and signed the consent form, the GEFT paper-and-pencil test was administered aiming to highlight the participants' cognitive characteristics. After the participant solved the GEFT test, the GEFT score of him was calculated. Depending on his score, the participant was classified as FD or FI.

Phase B: The participant was instructed to wear the smartwatch on the hand he usually wears one in order to feel comfortable. The participant had to create two kinds of passwords (PIN-based password and picture password). First, he was asked to create a PIN-based password and confirm it. Then he was asked to login with the same password that he created to be able to see his heart rate on that moment. Afterwards he had to create the other kind of password (graphical) but in order to familiarize himself with this kind of password he performed a training session. Data in this session was not collected. This training session could be repeated as many times as desired, so that the user was able to create a picture password. After, the participant familiarized himself with this approach, he was asked to create a picture password and then login with it in order to access his heart rate again. All participants performed these steps on the same smartwatch. Also, each participant was required to enter the password as fast as possible

during each step because data were implicitly collected and tracked for further empirical analysis.

Phase C: Once the phase B was completed, a post-study online questionnaire was conducted and each participant was asked to fill it out. So, various qualitative data were collected. Participants were asked on the strategies they followed during password creation and their perception of the security and usability of the two authentication schemes. The online questionnaire was designed using Google forms and it can be found in the appendices of this thesis. Overall, the study lasted about half an hour for each user. The empirical study was finished by thanking each participant for his participation.

5.5 CONCLUSION

In this chapter the process of the evaluation study has been analyzed. All users were classified to FD or FI. Furthermore, they have been familiarized with picture password and after that, they have created a PIN-based password and a picture password.

CHAPTER 6

6 ANALYSIS OF RESULTS

6.1 INTRODUCTION

This chapter presents in detail the results and analysis of the data collected from the evaluation study described in Chapter 5.

6.2 REGISTRATION PHASE

i. Time to create the password: The creation time is the duration it takes to a participant to register in milliseconds. Registration is completed when the user enters his password and confirms it correctly. For both password schemes (PIN-based password & Picture password) the creation time is measured by summing the user's time in the "Create" screen and in the "Confirm" screen.

PIN-based password scheme: The data shows that users' field dependence-independence affected the time needed to register with PIN-based password, with FD users being faster than FI users by 2.8 seconds.

Picture Password scheme: Furthermore, users' field dependence-independence affected the time needed to register with picture password, with FI users being faster than FD users by 1.4 seconds.

PIN-based password scheme Vs Picture Password scheme: The authentication schemes (PIN vs. picture) has a main effect on creation time. FD users were significantly faster by 1.2 seconds in register on PIN password compared to picture password. Also significant differences were observed between the two authentication schemes for FI users. FI users were faster by 3.0 seconds in register on picture password compared to PIN password. Thus, FD users were more efficient in register through PIN password scheme than picture password scheme, while for FI users the opposite happens.

	PIN-based password		**Picture Password**	
	FD	**FI**	**FD**	**FI**
Mean	12905	15757	14079	12673
SD	6452,60	8552,54	7714,45	4337,32

Table 6.1: Mean and standard deviation (SD) of registration time (in milliseconds) for FD-I between the two authentication schemes

ii. Retries: Retries are the set of repetitions made by a user. If a user created his password immediately then he has not made any repetition. But if he created his password by the second attempt this means that he had one retry.

PIN-based password scheme: In this scheme significant difference was found in the number of retries between the FD and FI users. Two of the FI users did not register immediately but they needed one retry each, in order to create correctly their password, while the FD users were able to create their password from the first attempt.

Picture Password scheme: In this scheme, the analysis revealed that the effect of field dependence-independence on retries was not significant. This happens because two FD and two FI participants needed repetitions to create their password. The first FD user made one repetition but the second FD user made two repetitions to complete the creation process. In contrast, the two FI users needed only one retry in order to create correctly their password.

PIN-based password scheme Vs Picture Password scheme: The total number of retries to register a new password was less in PIN-based password scheme than picture password scheme. The effect of user authentication type on retries for FI users was not significant. This is because the number of FI's retries were the same both in PIN-based password and picture password. Contrariwise the statistics show that FD users had more repetitions on picture password scheme than PIN-based password scheme. Nevertheless, the total number of retries made by the participants regardless of the effect of field dependence independence and authentication type was quite low (with only 50 participants).

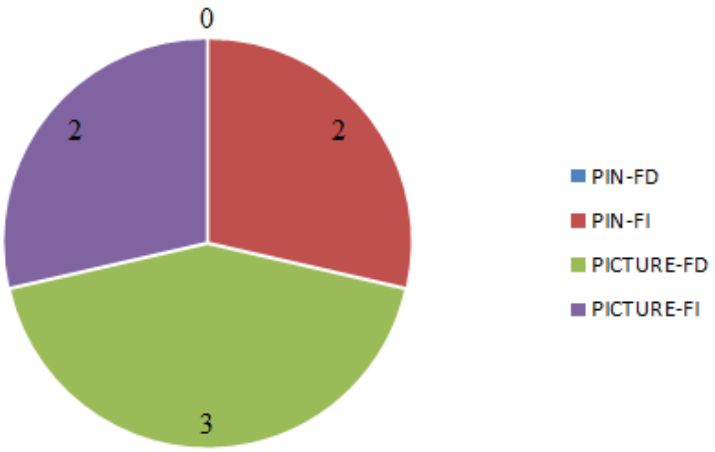


Figure 6.1: Number of retries made by the users to create their password

iii. Successful create: Successful create means that users have successfully created their password, no matter how many retries they have made. Unsuccessful creation means that despite the repetitions, the user was unable to create his password.

Data shows that users' field dependence-independence and the user authentication type did not affect the successful creation of users' password. All 50 participants managed to create both the PIN-based password and picture password successfully.

iv. The location of the clicks for Picture Password: The users' clicks on picture password scheme mostly rely on the hotspots (Points of Interest-PoIs) of the picture. A point of interest is a standout region in a picture. Three popular ways that users used to

identify standout regions are finding regions with semantic-rich meanings (objects), such as face, eyes or car, finding regions with remarkable shapes (line, rectangle, circle) and finding regions with outstanding colors (red, green, blue). It is the best if the locations of users' clicks follow a uniform distribution on the picture. However, such passwords would be difficult to remember by users [5].
By analyzing the collected passwords, I notice that also in this picture password scheme users chose standout regions on which to click. Minimal users claimed to choose locations randomly without caring about the background picture. Analyzing the attributes and the patterns of PoIs that users preferred to click, I found that they clicked on the mountain on top left, on the sun and on the two mountains on top right. Other locations that attracted users to click included the egg on bottom right, the plain on the center, the trees on the left and the lake on the bottom. It was found that the users tended to choose similar PoIs.

Below is the analysis of the points that FD and FI users clicked for each of the five gestures.

Gesture 1: We notice that for the first gesture, both types of users (FD & FI) have focused on the points that located on the top half of the image. We see that most of the users have clicked on the mountain on the top left. We also notice that several FI users have clicked on the egg and the sun while few FD users have chosen these points. None FD user has clicked on the plain on the center of the image and on the two mountains on the top right, while we observe that some FI users have clicked on these points. (Figure 6.2, Figure 6.3)

The attention of the users was drawn by the points of interest located at the top of the image. That's why the most of them selected the mountain on top left, which is the first point of interest, after scanning a very small part of the image. FD users mainly focused on the top half of the image, as there was a lot of visual information they had to explore. In their eyes, the whole image was seeking their attention and given their inherent difficulties in exploring visually complex scenes, they limited their search activity at the top half of the image. For this reason only a minority of them clicked on the egg and on the sun. FI users focused also on the top half of the image, that immediately caught their

attention, but rather than clicking on those points right away, they explore some other options before deciding on which points they would click. For this reason some FI users who did not click on the mountain on top left, they chose to click on the egg or on the sun or on the plain or on the two mountains on the top right to create their password.

Figure 6.2: Gesture 1 of FDs

Figure 6.3: Gesture 1 of FIs

Gesture 2: On the second gesture, we notice that most users have chosen a point that is also located on the top of the image. However, they have not chosen the same point that they had previously chosen, namely the mountain on the top left. Now they have selected the objects on the top center and on the top right of the image, namely the sun and the two mountains respectively. Additionally, we see that many of the FI users have selected the egg as opposed to the FD users where few have chosen it. (Figure 6.4, Figure 6.5)

The unique characteristics of the FD and FI individuals influenced the strategy they followed to the second click. FD users as before explored a very small number of points located mainly at the top half of the image. That's why the most FD users did not click on the egg which is on the bottom right. FI users, observing their behavior, they explored the image at first and then they decided on how they would make their clicks. Thus, some of the FI users left from the top of the image and went to the bottom by choosing to click on the egg. A possible explanation for why they did not choose the same point as before is that they tried to create a strong password. The most users

clicked on the top center or on the top right part of the image because they started scanning the image from the top half and their glance went from left to right.

Figure 6.4: Gesture 2 of FDs

Figure 6.5: Gesture 2 of FIs

Gesture 3: On the third click, most FD users have stayed at the top of the image as before. We see that FD users have not made any clicks on the sun which they had done before. The most have focused on the two mountains on the top right. As for FI users, most have also been focused on the mountains on the top right too but many of them have done other clicks. For example, they clicked on the mountain on the left, on the sun, on the egg, on the lake and on the plain. (Figure 6.6, Figure 6.7)

FI individuals, due to their analytic nature are more likely to explore the whole image, while FD individuals with the difficulty in exploring complex images they limited their field of view to the top of the image. This may be the reason that the most FDs made a click on the two mountains on the top right, while the FIs focused on more points of interest. Also, users have clicked on the two mountains on the top right, perhaps because they are the third successive point of interest at the top of the image, since as we have seen, they scan the image from the top to the bottom, going from left to right.

Figure 6.6: Gesture 3 of FDs

Figure 6.7: Gesture 3 of FIs

Gesture 4: In the fourth click, we see that the attention of most FDs and FIs has been centered mainly on the egg which is located on down right of the image. Also, several users focused on the right mountain of the two mountains on the top right. At the same time, however, we notice that there are users who have clicked on other points of interest. (Figure 6.8, Figure 6.9)

Users began to observe the image from top left, moved their look right and then right down. There are also users who considered the two mountains on the right as one point of interest and users who saw them as two separate points of interest. So those who saw the two mountains as one point of interest clicked on the egg because in the way they observe the image, the egg is the fourth consecutive point of interest. While those who considered the two mountains as two separate points of interest, they clicked on the right mountain because for them that is the fourth consecutive point of interest. The above reasons are a possible explanation for the fact that most users have clicked on the egg and several users on the second mountain on the right. As mentioned above users observed the image in a circular way (from the top left, they moved their gaze right and then immediately down). This may have happened because users were interacting with a smartwatch that has a small screen size and so easily their look could move from the top of the image to the bottom. But if this study was not done on smartwatch but on a device with larger screen, maybe the way the users would observe the image was different from the way they observed it now. For example, they might have moved their

eyes constantly from left to right, starting from the top of the image and going down to the bottom.

Figure 6.8: Gesture 4 of FDs

Figure 6.9: Gesture 4 of FIs

Gesture 5: In the fifth click, we observe that several FDs and FIs have clicked on the egg while the most users focused on the center of the image. The users who focused on the center of the image, we notice that they clicked to random points and not on points with some semantic meaning (POI). (Figure 6.10, Figure 6.11)

The users who saw the two mountains on the top right as one point of interest, for their fifth gesture, they clicked on the center of the image. A possible explanation is that they have already clicked on the hotspots and for their last click they maybe decided to click randomly to the center of the image. While those who considered the two mountains as two separate points of interest, they clicked on the egg because for them that is the fifth consecutive point of interest, in the way they have observe the image.

Figure 6.10: Gesture 5 of FDs

Figure 6.11: Gesture 5 of FIs

v. Password strength: The strength of the passwords created for each scheme, was measured in terms of number of guesses needed to crack each password. Thus, a brute force approach was used. For the PIN-based password scheme, it checks of all possible password combinations comprising of six digits starting from the number 0 to number 9 (e.g. 000000, 000001, 000002...) until it matches correctly with the password. For the picture password scheme, it checks of all possible password combinations comprising of five segments starting from segment 1 to segment 16 (e.g. 11111, 11112, 11113...) until it finds the password. It should be noted that all combinations produced by the PIN-based password scheme are 1,000,000 while all combinations produced by the picture password scheme are 1,048,576.

PIN-based password scheme: The effect of FD-I revealed a statistically significant difference in practical password strength for PIN-based password, with mean password strength 400487 for FIs and 464080 for FDs. So, more guesses were required to crack FDs' PIN-based passwords than FIs' PIN-based passwords.

Picture Password scheme: The results of the study suggest that the different human cognitive strategies affect the picture passwords' strength. The security strength of picture password for FI group was higher than FD group. FIs' passwords required 35389 more guesses to be cracked than FDs'. A possible explanation for this fact is that FIs followed an analytic approach to explore the image, thus they focused on more points than FDs who were frustrated by the number of POIs of the image.

PIN-based password scheme Vs Picture Password scheme: The kind of authentication scheme has a main effect on password strength for FDs and FIs. The analysis revealed that FI individuals created stronger PIN-based passwords, in terms of guessability, than picture passwords. Maybe they have focused on the POI so they did not click elsewhere. Perhaps that's why they've created a stronger PIN-based password. Furthermore, the analysis of the strength of the passwords created by FDs revealed that they have also created more difficult to guess PIN-based passwords than picture passwords. This happened because on picture password they explored a very small part of the image located mainly at the top half and so they decreased the probability of selecting stronger passwords. Also, FDs were overwhelmed with the number of POIs available and the holistic approach they followed did not help them create strong picture passwords.

Thus, both FD and FI groups created stronger PIN-based passwords than picture passwords.

	PIN-based password		Picture Password	
	FD	**FI**	**FD**	**FI**
Mean	464080	400487	384434	419823
SD	298583,50	318533,01	323193,82	319740,38

Table 6.2: Mean and standard deviation (SD) of password strength for FD-I between the two authentication schemes

6.3 AUTHENTICATION PHASE

i. Time to Login: The login time is the duration it takes to a participant to authenticate himself in milliseconds. An authentication attempt which fails (e.g. due to incorrect password) does not finish the login timer. The participant has to retry until he authenticates successfully or until the instructor interrupts him.

PIN-based password scheme: The data shows that users' field dependence-independence affected the time needed to authenticate with PIN-based password, with FI users being faster than FD users by 1 second.

Picture Password scheme: Furthermore, users' field dependence-independence did not affect much the time needed to authenticate with picture password. However FI's performance was better than FD's (FI: SD = 1378.34 Vs FD: SD = 1608.11).

PIN-based password scheme Vs Picture Password scheme: The authentication schemes (PIN vs. picture) has a main effect on login time. FD users were faster by 1 second in login with picture password compared to PIN password. Also, no significant differences were observed between the two authentication schemes for FI users. However FI's performance were better in authenticating with picture password than with PIN password (Picture password: SD = 1378.34 Vs PIN-based password: SD =2198.74).

Thus, both FD and FI users were more efficient in authenticating through picture password scheme than PIN-based password scheme.

	PIN-based password		Picture Password	
	FD	**FI**	**FD**	**FI**
Mean	6368	5329	5183	5119
SD	3181,61	2198,74	1608,11	1378,34

Table 6.3: Mean and standard deviation (SD) of login time (in milliseconds) for FD-I between the two authentication schemes

ii. Trials: Trials are the total number of attempts in order to login. If a user logged in immediately then he has done one trial. But if he logged in by the second attempt this means that he had two trials.

PIN-based password scheme: In this scheme significant difference was found in the number of trials between the FD and FI users. One FI user needed two trials in order to authenticate and another FI user logged in by the fourth trial, while three of the FD users needed two trials to logged in and one FD needed three trials. All other users were logged in from the first trial.

Picture Password scheme: In this scheme, the analysis revealed that the effect of field dependence-independence on trial was not very important. This happens because three FD and three FI participants logged in by the second trial. Also there is an FI user that needed three trials in order to authenticate successfully. Everyone else was logged in from the first trial.

PIN-based password scheme Vs Picture Password scheme: The total number of trials to login with PIN-based password scheme was approximately the same with the trials needed to log in with picture password scheme. The effect of user authentication type on trials for FI users was a little important. This is because the FI's trials with PIN-based password were less than the trials that they made with picture password. Contrariwise the statistics show that FD users had more trials on PIN-based password scheme than picture password scheme. Nevertheless, the total number of trials made by the users

regardless of the effect of field dependence independence and authentication type was quite low (with only 50 participants).

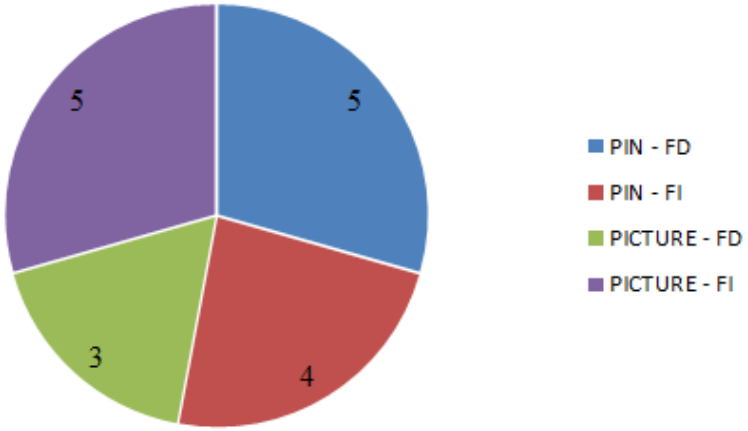


Figure 6.12: The additional trials made by users to login successfully

iii. Successful login: Successful login means that the users have successfully logged in, no matter how many trials they have made. Unsuccessful login means that despite the trials, the user was unable to login.

Data shows that users' field dependence-independence and the user authentication type did not affect the successful login by users. All 50 participants managed to login both with the PIN-based password and with the picture password successfully.

6.4 QUALITATIVE DATA - QUESTIONNAIRE

After the end of phase B, users responded to a questionnaire in order to collect a variety of qualitative data. Initially, only 5 out of 50 users had previously used smartwatch. Everyday more than 90% of the users are using a laptop and smartphone, 54% have responded that they are using a desktop computer while 30% are using a tablet. Moreover, 31 participants have said that it was quite easy to create the picture password, while 6 participants have struggled a little. As for the rest participants, they said they found neither easy nor difficult to create the picture password. Then users were asked about how they created their own picture password, that is, how they chose the points where they would make each click. Several users (58%) have said that they

try to find locations where special objects are, while 36% responded that they try to find locations where some special shapes are. Finally, 12 users have said that they try to find locations where colors are different from their surroundings and that they randomly choose a location to click without thinking about the background image. Users are then asked if they used a technique (e.g. use of birth dates) to remember the PIN-based password they created. Only a small minority (8 users) said they did not use any technique to remember their PIN-based password, while everyone else (42 users) had used a specific technique. Most users have used birth dates or another date which is special for them. Several users have used a part of their phone number or a pattern (such as numbers which are in a line, a virtual pattern, pressing one specific digit six times or two digits three times or pressing only even numbers). Other users put their ID number or a password that they already have. Furthermore, 76% of the participants said that they tried to do something which they found difficult, while the 24% did not find anything difficult. Users found it difficult to interact with smartwatch because of its small screen and their large fingers and they said that the tapping was not very accurate. Also, in PIN-based password they face a difficulty because the buttons were small. Some other users had a difficulty with the picture password, for instance to find the same points in the image. Finally, some people struggled with the GEFT test, as well, they face difficulties with retries of passwords and they said it was hard to remember the passwords they entered. Additionally, 60% of the participants prefer to login with PIN-based password in smartwatches, while 40% prefer to login with picture password. Finally, 64% of users answered that they think that the picture password is more secure than a PIN-based password, while 36% disagreed with this statement.

6.5 USABILITY AND SECURITY ANALYSIS OF THE SCHEMES

6.5.1 Usability Analysis

The ISO defines usability as the "effectiveness, efficiency and satisfaction with which a specified set of users can achieve a specified set of tasks in a particular environment" [38]. The study reported investigated the usability of the two password schemes.

In this research, effectiveness is interpreted as the ability of reproducing passwords correctly and it was measured as the number of attempts the participants took to enter passwords correctly (i.e. retries - for registration phase, trials - for authentication phase). Effectiveness is the most important usability factor. If users are not able to authenticate, the concept is not feasible. A system with lesser attempts indicates good effectiveness. The analysis revealed that users needed less retries in registration phase with PIN-based password than with picture password (PIN: retries = 2, PICTURE: retries = 5). Moreover, in authentication phase, less trials were caused with picture password than with PIN-based password (PIN: trials = 9, PICTURE: trials = 8). However, the analysis revealed that these differences were not significant.

Efficiency was confirmed as a crucial usability factor as poor efficiency makes authentication concepts unfeasible. In this study, efficiency is defined in terms of mean registration time and the time taken for successful authentication attempts. The analysis revealed that users were overall significantly faster in completing the registration task of picture password than PIN-based password (PIN: mean registration time = 14730ms, SD = 7980, PICTURE: mean registration time = 13179ms, SD = 5824). Furthermore, in PIN-based password scheme, users needed a little longer to complete the authentication task than in picture password scheme (PIN: mean authentication time = 5703ms, SD = 2643, PICTURE: mean authentication time = 5142ms, SD = 1466).

Satisfaction was measured as the users' experiences of using the graphical authentication scheme. To understand user experience, a question was asked in the questionnaire. The question was "Do you like graphical passwords as an alternative authentication method in smartwatches?" Most users (72%) stated that they liked graphical passwords as an alternative authentication method in smartwatches, thus they were satisfied about it.

6.5.2 Security Analysis

The security analysis of the created passwords in this study was measured in terms of password strength. Password strength is traditionally defined by the chance that a password is guessed by an attacker. So, the users' passwords should be strong enough to

guessing attacks. Password guessing attacks can be classified into two: brute force attack and dictionary attack. This analysis has been focused on brute force attack. For PIN-based password, we observed that FD individuals created stronger passwords than FI individuals. Contrariwise, for picture password we see that the security strength of FI group was higher than FD group, so FIs' picture passwords required more guesses to be cracked than FDs'. Furthermore, the kind of authentication scheme has played an important role for password strength of FDs and FIs. For FI individuals, we observed that they created stronger passwords with PIN-based password scheme than with picture password scheme. Furthermore, the analysis revealed that FDs have also created more difficult to guess passwords with PIN-based password scheme than picture password scheme.

The security of picture password schemes mostly relies on the location distribution of users' gestures. A background picture affects the user choice in gesture location. Users are likely to choose POIs on a picture when selecting a password. Thus, the POIs of a picture may decrease a user's password space by directing them toward specific gestures. So, a brute force algorithm centered on this notion (POIs) will assist in attacking a password for a previously unseen picture. Consequently, the POIs of an image can reduce the feasible password space tremendously.

To understand the users' perceived security of the two authentication schemes, a question was asked in the questionnaire. The question was "Do you think picture passwords are more secured than PIN-based passwords?" The majority of the participants (64%) believed that the picture password scheme offers better security than PIN-based password scheme.

6.6 CONCLUSION

This chapter analyzed and discussed the results of the evaluation study conducted to evaluate the usability and security aspects of the PIN-based password scheme and picture password scheme. The study design allowed collecting quantitative performance data and qualitative feedback. The next chapter presents the overall conclusion of the thesis as well as the limitations of the study and future researches.

CHAPTER 7

7 CONCLUSIONS AND FUTURE WORK

7.1 CONCLUSION OF THESIS

This thesis investigates both forms of knowledge-based authentication which are PIN-based password and graphical password. The password of PIN-based authentication scheme is consisted of six digits from zero to nine. In addition, the graphical password is based on the cued-recall authentication scheme in which a user is presented with a background image and he has to click on five points in a sequence. A prototype of the two authentication schemes was implemented on a Fitbit versa smartwatch.

First of all, in order to investigate the aims and objectives of the thesis, a user experiment has been conducted with fifty participants. Also, I have analyzed and summarized the security and usability aspects of the presented user authentication schemes based on widely applied security and usability metrics found in the literature. The results of this study pointed out that the human cognitive factors affect the time to enter the passwords and also the passwords' strength. Concerning the authentication time with PIN-based password, FI users were faster than FD users. Also, with picture password scheme FI's performance was better than FD's. Overall, with PIN-based password scheme users needed a little longer to complete the authentication task than with picture password scheme. About password strength, in PIN-based authentication scheme FDs created stronger passwords than FIs. Contrariwise, the security strength of picture password scheme for FI group was higher than FD group. Briefly, the users created stronger passwords with PIN-based authentication scheme than with picture password scheme.

Furthermore, the results suggest that FD-I cognitive style of users influenced the strategy they followed to create their passwords. In picture password scheme, all the

users mainly choose from among the POIs to perform their clicks. FD users have identified about the same POIs as FI users. I noticed that all users started exploring the image from the top left. FD users in their first clicks selected POIs that were placed at the top of the image and on the fourth/fifth click were able to analyze the bottom of the image and click on it. Therefore, FD users were late to analyze the bottom part of the image. Instead, I noticed that FI users analyzed the entire image and the bottom part of it from their first clicks and so they clicked to the whole image from the beginning. In both groups (FD and FI) I noticed that their clicks followed a circular path. That is, they clicked starting from the top left, going on top right, then right down and finally center. Despite the difference in users' cognitive features, we see this common path perhaps because they interacted with smartwatch. The smartwatch screen is too small and therefore the image is small. So although FD users have a more holistic nature it was easier to direct their eyes across the image (and to the bottom part) because of its small size. If the experiment was conducted on a larger screen size device, FD users could only focus on the top of the image due to their features while FI users may have analyzed the whole picture because of their analytical nature. Generally, both FDs and FIs made moves across the picture, but FD focused on its top.

Users tend to choose and click on predictable areas or spots of the picture. This creates "hot-spots" which is a well-known weakness in the picture password scheme. POIs on a picture may decrease a user’s password space by steering them towards specific gestures. Users also tend not to choose blank areas, such as clear sky regions. This makes the password space to become smaller. POIs narrow the search space for the attacker and a brute force algorithm centered on this notion can crack a password for a previously unseen picture [5].

To sum up, traditional PIN-based passwords are vulnerable to brute-force and dictionary attacks as users choose weak and predictable passwords in favor of memorability. On the other hand, graphical passwords are vulnerable to POIs brute-force attack. Results showed that graphical authentication has a high usability and it is likely to replace PIN-based authentication methods in the near future. And even today, we can see graphical passwords being used in Windows10 OS as an alternate to text password. So with the advancement in technology mainly in touch based technology,

graphical authentication plays a very promising role for various authentications in such devices or gadgets.

7.2 LIMITATIONS

While the apps show that they can run on a smartwatch nicely, they still have some limitations. They were only tested on a Fitbit versa device. I suspect the apps will behave similarly on Fitbit Ionic, but could well have some display issues as the Ionic has a different size screen. Another limitation concerns that I used GEFT test to classify an individual as either FD or FI. Considering that the GEFT test highlights cognitive differences along a continuum scale, the use of a cut-off score might not classify correctly individuals that fall in between the two end points (e.g. Field-mixed [Angeli et al., 2009]). In addition, the graphical authentication scheme is not safe from shoulder surfing problem. Based on the literature survey of various graphical schemes, it is evident that a system that claims to have no shoulder surfing problem, has more complications in its authentication method and that the usability is dramatically decreased. Thus, in order to maintain the ease of use I have not looked into the shoulder surfing prevention mechanisms. Finally, even though the participants did not use their own credentials, it is very likely that most participants were trained with PIN-based password and actively used various PINs on a daily basis (e.g. ATM). On the contrary, I cannot assume that all participants had gained previous experiences with picture password. These differences may have influenced both the performance and the perception of the tested concepts.

7.3 FUTURE WORK

As of now graphical authentication still needs a lot of research in order to be deployed in a large scale environment and also the problem of shoulder-surfing needs to be looked. Another future work can be the development of an algorithm that performs a brute-force attack on POIs and calculates the number of guesses to crack graphical passwords. Also, as there is yet no wide deployment of graphical password systems, the vulnerabilities are yet to be exploited. Much more user studies and research are

necessary for graphical user authentication methods to achieve higher levels of usefulness.

BIBLIOGRAPHY AND REFERENCES

[1] Marios Belk, Christos Fidas, Christina Katsini, Nikolaos Avouris, George Samaras. (2017). Effects of Human Cognitive Differences on Interaction and Visual Behavior in Graphical User Authentication. INTERACT 2017.

[2] Chris A. Chinien, France Boutin. (1993). Cognitive Style FD/I: An Important Learner Characteristic for Educational Technologists.

[3] Christina Katsini, Christos Fidas, Marios Belk, Nikolaos Avouris, George Samaras. (2017). Influences of Users' Cognitive Strategies on Graphical Password Composition.

[4] Belk, Marios, Fidas, Christos, Germanakos, Panagiotis and Samaras, George. (2017). The Interplay between Humans, Technology and User Authentication: A Cognitive Processing Perspective. Computers in Human Behavior.

[5] Ziming Zhao, Gail-Joon Ahn, Jeong-Jin Seo. (2013). On the Security of Picture Gesture Authentication. 22nd USENIX Security Symposium.

[6] Fitbit Versa Health and Fitness Smartwatches. Retrieved from https://www.fitbit.com/eu/shop/versa

[7] FITBIT VERSA SMARTWATCH. Retrieved from https://www.smartwatchspecifications.com/Device/fitbit-versa-smartwatch/

[8] Fitbit Versa. Retrieved from https://www.smartwatchspex.com/fitbit-versa-specs/

[9] Fitbit Versa. Retrieved from https://www.walmart.com/ip/Fitbit-Versa/673273964

[10] Fitbit Versa review: Finally, a smartwatch that can make Fitbit proud. Retrieved from https://www.zdnet.com/product/fitbit-versa/

[11] JavaScript. Retrieved from https://developer.mozilla.org/en-US/docs/Web/JavaScript

[12] JavaScript Guide. Retrieved from https://dev.fitbit.com/build/guides/user-interface/javascript/

[13] Cascading Style Sheets. Retrieved from https://en.wikipedia.org/wiki/Cascading_Style_Sheets

[14] CSS Guide. Retrieved from https://dev.fitbit.com/build/guides/user-interface/css/

[15] Scalable Vector Graphics. Retrieved from https://en.wikipedia.org/wiki/Scalable_Vector_Graphics

[16] SVG Components Guide. Retrieved from https://dev.fitbit.com/build/guides/user-interface/svg-components/

[17] Samsung Galaxy Note II N7100. Retrieved from https://www.gsmarena.com/samsung_galaxy_note_ii_n7100-4854.php

[18] Samsung Galaxy Note II GT-N7100 - 16GB - Titanium Gray (Unlocked) Smartphone. Retrieved from https://www.ebay.com/p/Samsung-Galaxy-Note-II-GT-N7100-16GB-Titanium-Gray-Unlocked-Smartphone/127234995

[19] L. O'Gorman. (2003). Comparing passwords, tokens, and biometrics for user authentication. Proceedings of the IEEE, Vol. 91.

[20] Xiaoyuan Suo, Ying Zhu, G. Scott. Owen. (2005). Graphical Passwords: A Survey. Paper presented at Annual Computer Security Applications Conference: ACSAC, Los Angeles. Georgia State University.

[21] Angeli, C., Valanides, N., & Kirschner, P. (2009). Field dependence-independence and instructional-design effects on learners' performance with a computer-modeling tool. Computers in Human Behavior.

[22] Hong, J., Hwang, M., Tam, K., Lai, Y., & Liu, L. (2012). Effects of cognitive style on digital jigsaw puzzle performance: A GridWare analysis. Computers in Human Behavior.

[23] Herman, Witkin, A., Carol Ann Moore, Donald, Goodenough, R., Patricia Cox, W. (1975). Field Dependent and Field-Independent Cognitive Styles and their Educational Implications. ETS Research Bulletin Series 2.

[24] Witkin, H.A., Oltman, P., Raskin, E., & Karp, S. (1971). A manual for the embedded figures test. Palo Alto, CA: Consulting Psychologists Press.

[25] Anil Jain, Ruud Bolle, and Sharath Pankanti. (1999). Biometrics: Personal Identification in Networked Society. Kluwer Academic Publishers.

[26] I. Jermyn, A. Mayer, F. Monrose, M.K. Reiter, and A. Rubin. (1999). The Design and Analysis of Graphical Passwords. In Proc. of the 8th USENIX Security Symposium.

[27] Art Conklin, Glenn Dietrich, and Diane Walz. (2004). Password-based authentication: A system perspective. In 37th Hawaii Int. Conference on System Sciences.

[28] Emanuel von Zezschwitz, Alexander De Luca, Bruno Brunkow and Heinrich Hussmann. (2015). SwiPIN: Fast and Secure PIN-Entry on Smartphones. In Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI'15). ACM, NewYork, USA.

[29] X. Suo, Y. Zhu and G. Owen. (2005). "Graphical Passwords: A Survey", In Proc. ACSAC.

[30] G.Blonder. (1996). Graphical Password. In Lucent Technologies.

[31] S. Wiedenbeck, J. Waters, J.-C. Birget, A. Brodskiy and N. Memon. (2005). "Authentication using graphical passwords: Effects of tolerance and image choice", in Proceedings of the 2005 symposium on usable privacy and security, ACM.

[32] A. Paivio, T. B. Rogers and P. C. Smythe. (1968). Why Are Pictures Easier to Recall Than Words? Psychonomic Science.

[33] Nur Haryani Zakaria, David Griffiths, Sacha Brostoff and Jeff Yan. (2011). Shoulder Surfing Defence for Recall-based Graphical Passwords. In Proceedings of the Seventh Symposium on Usable Privacy and Security (SOUPS '11). ACM, NewYork, NY, USA.

[34] Hai Tao and Carlisle M. Adams. (2008). Pass-Go: A Proposal to Improve the Usability of Graphical Passwords. I. J. Network Security 7.

[35] Susan Wiedenbeck, Jim Waters, Jean-Camille Birget, Alex Brodskiy and Nasir Memon. (2005). PassPoints: Design and longitudinal evaluation of a graphical password system. International Journal of Human-Computer Studies 63. HCI research in privacy and security.

[36] Sacha Brostoff and M. Angela Sasse. (2000). Are Passfaces More Usable Than Passwords? A Field Trial Investigation. In People and Computers XIV — Usability or Else!,Sharon McDonald, Yvonne Waern and Gilbert Cockton (Eds.) Springer London,London.

[37] Passfaces. (2018). Passfaces: Two Factor Authentication for the Enterprise.

[38] Human-Computer-Interaction. Retrieved from https://wiki.typo3.org/Human-Computer-Interaction

[39] How to run a WebServer on Android. Retrieved from http://jensklin.triangulum.uberspace.de/how-to-run-a-webserver-on-android/?fbclid=IwAR2dfuDJtYwgPNBSavodgmrx8RIODPZvSvoixpymkPeu7C9HS9WhXnxvikw

APPENDIX A: INSTRUCTIONS FOR USE

- The Fitbit watch can only connect to open, WEP, WPA personal and WPA2 personal Wi-Fi networks and personal hotspot.

- Be sure that the Wi-Fi network that the smartwatch is connected to is the same with the Wi-Fi network that the phone is connected to.

  How to connect the smartwatch to the network that the phone is connected to:

  1 Open the Fitbit application on the phone.
  2 Press on the Fitbit versa icon.
  3 Scroll down until you find the “Wi-Fi settings”.
  4 Select the network that your phone is connected to.

- How to run the Fitbit applications:

  1. Open the Wi-Fi of the phone.
  2. Open the Bluetooth of the phone.
  3. Open the Fitbit application on the phone.
  4. Press on the Fitbit versa icon.
  5. Go to "Developer Menu".
  6. Enable the "System Location Permission".
  7. Go to the settings app on the smartwatch.
  8. Scroll down and tap to "Developer Bridge".
  9. Wait until "Connected to Server" is shown.
  10. Login to Fitbit Studio.
  11. How to run training app:
      a. Open the project "training" from the Fitbit Studio.
      b. Click to "Select a phone Select a device".
      c. Select your phone and smartwatch and wait until the green color appears.
      d. Click "Build".
      e. Click "Run".

      (App installed to the smartwatch)
  12. How to run pinbit and picbit apps:
      a. Open the android app with the Server.

b. Click the button "START" in order to make the Server running.
c. Open the project "pinbit"/"picbit" from the Fitbit Studio.
d. Click to "Select a phone Select a device".
e. Select your phone and smartwatch and wait until the green color appears.
f. Go to the folder "companion" and open the file "index.js" (companion/index.js).
g. In this file, go to the function "sendData_via_POST(type, data)".
h. Change the IP address of the line 34 and put the IP address that appears to the android app ("Server running at: 192.168.43.120:8765").
i. Click Build.
j. Click Run.

(App installed to the smartwatch)

- In order to make the pinbit and picbit apps to work right:
    1. Wait until this two lines appears to the console:
        a. Loaded and evaluated: file:///android_asset/bootstrap.js
        b. Loaded and evaluated: file:///data/user/0/com.fitbit.FitbitMobile/app_companions/b0b24173-a556-47b2-b739-336239f9b3fa/0x0de6a01797689419/companion.js
    2. If they are not appeared then press again the button "Run".
    3. If the message "Companion unloaded" appears to the console, then press again the button "Run".

APPENDIX B: CONSENT FORM

What this study is about

The purpose of this study is to understand how people interact with Graphical User Authentication (GUA) schemes. Your participation in this study will help us improve research in usability and security of GUA schemes.

Your participation in this study is voluntary

You can take a break at any time. Just tell the researcher if you need a break. You can leave at any time without giving a reason.

Information we want to collect

We will watch how you complete a GUA registration and login task and we will ask you to respond to some questions and a paper and pencil test. We will take notes to record your comments and actions.

How we ensure your privacy

We may publish research papers and reports that may include your comments and actions, but your data will be anonymous. This means your name and identity will not be linked in our research reports to anything you say or do.

Your consent

Please sign this form showing that you consent to us collecting these data.

I give my consent (please tick all that apply):

- ☐ For people to observe me during the research.
- ☐ For my interaction data to be tracked.
- ☐ For my responses to a questionnaire and a paper and pencil test to be recorded.

If you want to withdraw your consent in the future, contact the persons named below who will destroy any personal data we hold about you. Otherwise, we will delete your personal data after two years.

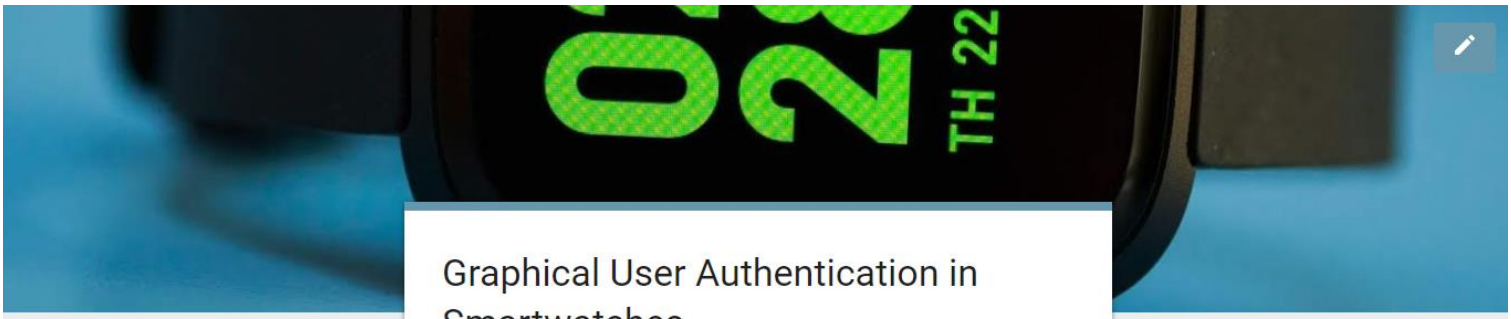
Eleni Katsi (ekatsi03@cs.ucy.ac.cy)
Marios Belk (mariosbelk@hotmail.com)

Participant Name _____

Signature _____

Date _____

APPENDIX C: QUESTIONNAIRE



Graphical User Authentication in Smartwatches

* Απαιτείται

1. Your user ID was: *

Η απάντησή σας

2. Was this your first time using a smartwatch? *

- ○ Yes
- ○ No

3. What other electronic devices do you use in your everyday life? *

- ☐ Desktop computer
- ☐ Laptop computer
- ☐ Smartphone
- ☐ Tablet

4. How difficult did you find the gesture creation? *

	1	2	3	4	5	
Very easy	○	○	○	○	○	Very difficult

5. Could you explain the way you choose locations to perform your gestures? *

- ☐ I try to find locations where special objects are
- ☐ I try to find locations where some special shapes are
- ☐ I try to find locations where colors are different from their surroundings
- ☐ I randomly choose a location to draw without thinking about the background picture

6. Did you use any special technique (e.g. use of birth dates) to help you create and remember your PIN? *

- ○ Yes
- ○ No

7. If yes, what was the special technique that you used?

Η απάντησή σας

8. Did you, at any point of the experiment, tried to do something which you find difficult to do? *

- ○ Yes
- ○ No

9. If yes, what was it?

Η απάντησή σας

10. Which authentication method would you prefer to login in smartwatches? *

- ○ PIN
- ○ Graphical Password

11. Which authentication method would you prefer to login in your everyday computer usage (e.g., emails, social networks, etc.) *

- ☐ PIN
- ☐ Text Password
- ☐ Graphical Password

12. Do you like graphical passwords as an alternative authentication method in smartwatches? *

- ○ Yes
- ○ No

13. Do you think picture passwords are more secure than PIN-based passwords? *

- ○ Yes
- ○ No

ΥΠΟΒΟΛΗ

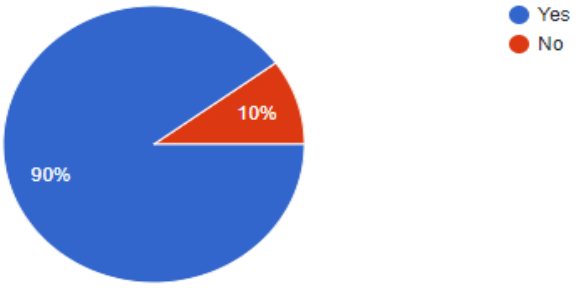
Μην υποβάλετε ποτέ κωδικούς πρόσβασης μέσω των Φορμών Google.

You can see the questionnaire on this link: https://goo.gl/forms/V31zuDELUL0Exn932

APPENDIX D: RESULTS OF QUESTIONNAIRE

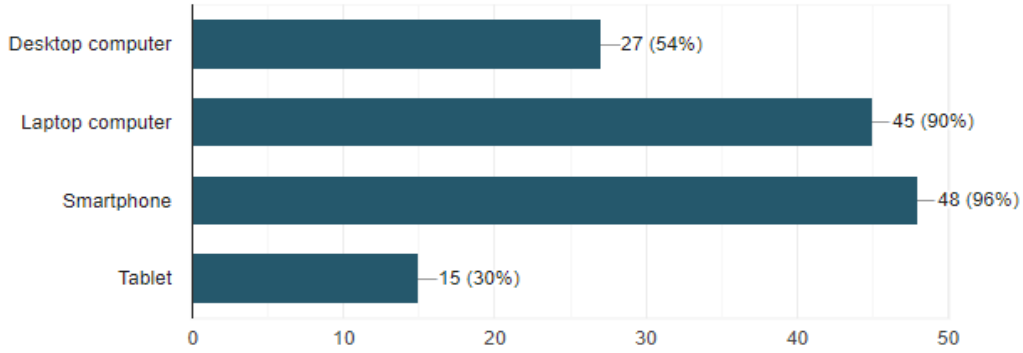
2. Was this your first time using a smartwatch?

50 απαντήσεις



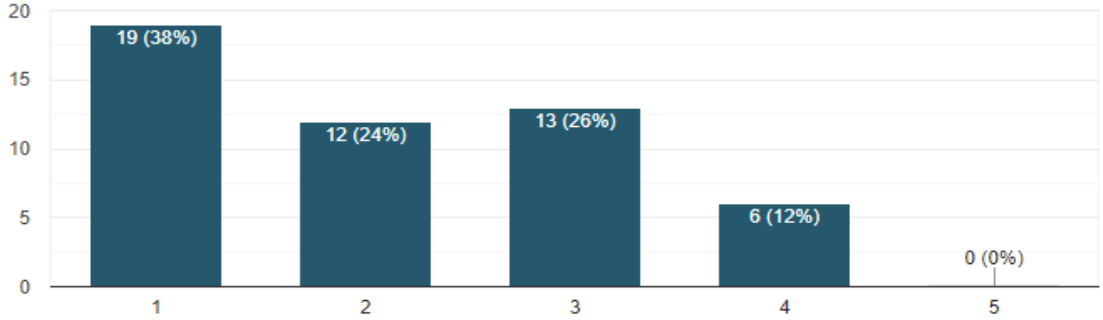
3. What other electronic devices do you use in your everyday life?

50 απαντήσεις



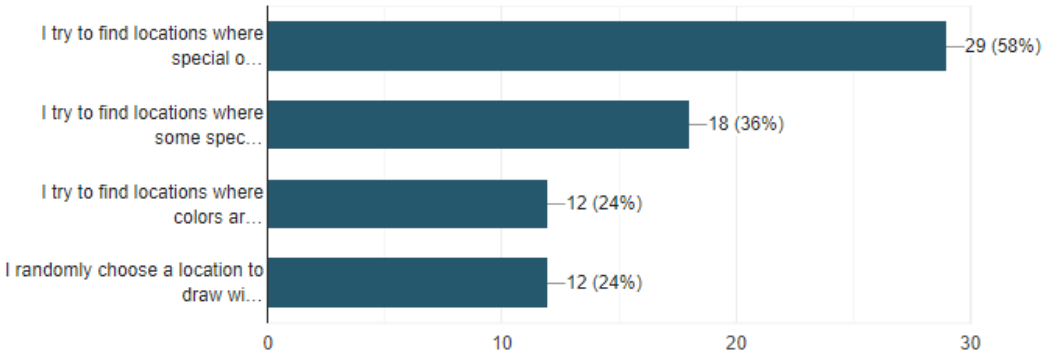
4. How difficult did you find the gesture creation?

50 απαντήσεις



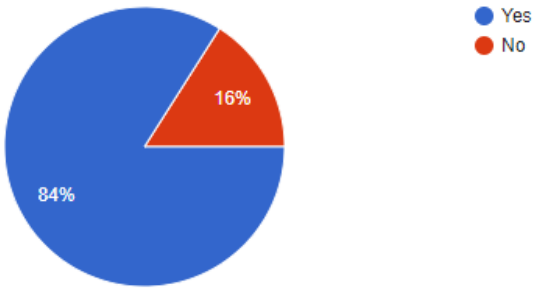
5. Could you explain the way you choose locations to perform your gestures?

50 απαντήσεις



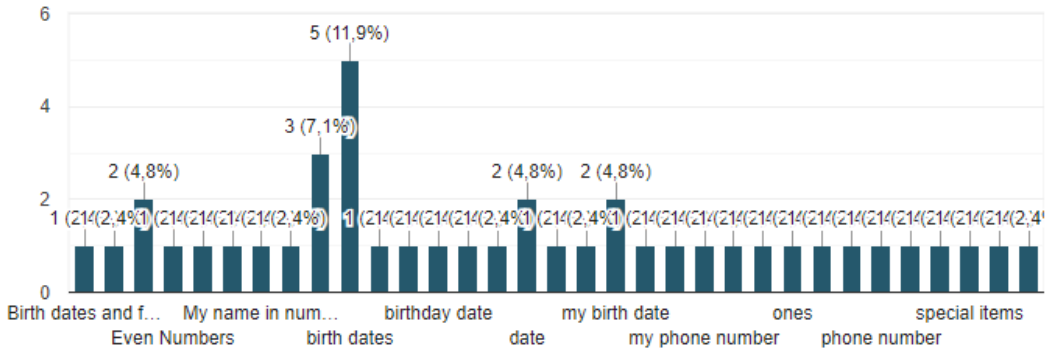
6. Did you use any special technique (e.g. use of birth dates) to help you create and remember your PIN?

50 απαντήσεις



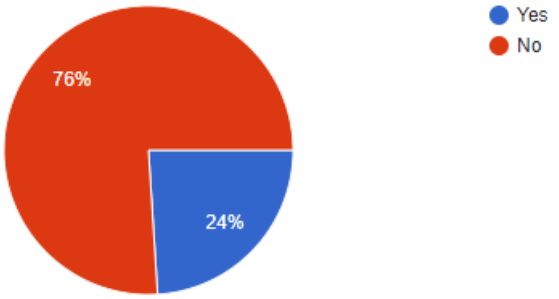
7. If yes, what was the special technique that you used?

42 απαντήσεις



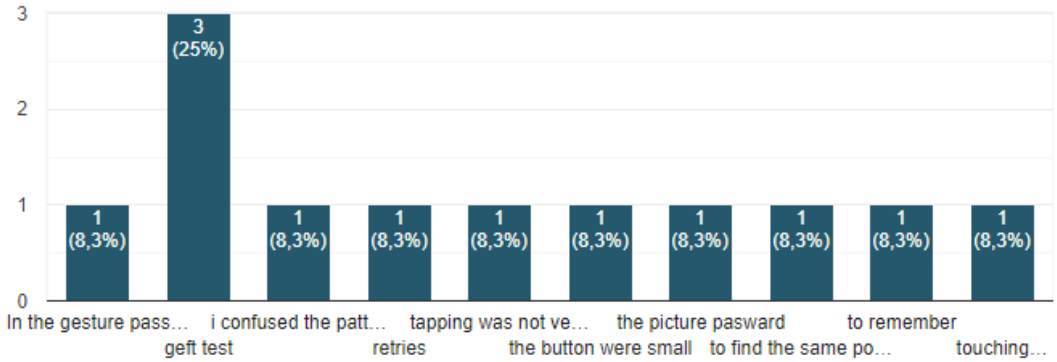
8. Did you, at any point of the experiment, tried to do something which you find difficult to do?

50 απαντήσεις



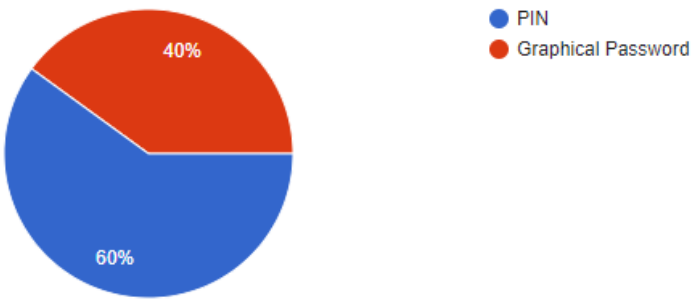
9. If yes, what was it?

12 απαντήσεις



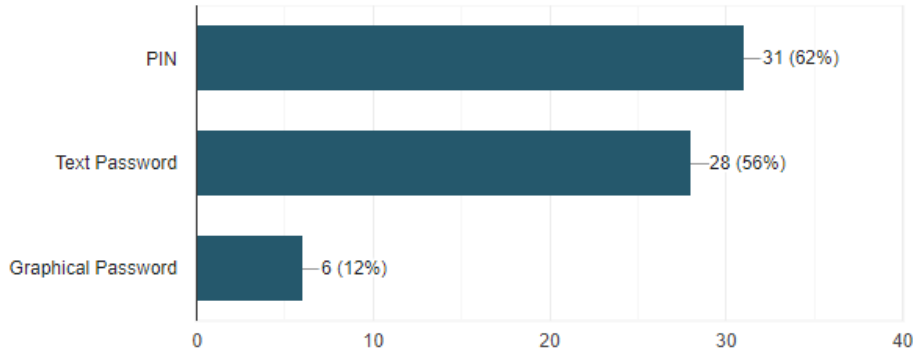
10. Which authentication method would you prefer to login in smartwatches?

50 απαντήσεις



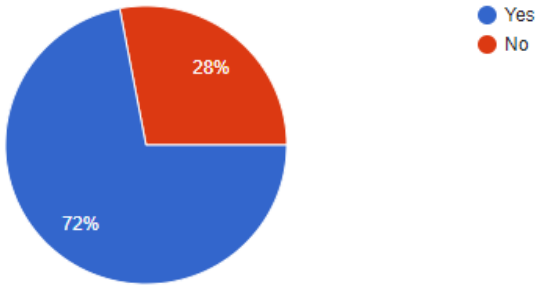
11. Which authentication method would you prefer to login in your everyday computer usage (e.g., emails, social networks, etc.)

50 απαντήσεις



12. Do you like graphical passwords as an alternative authentication method in smartwatches?

50 απαντήσεις



13. Do you think picture passwords are more secure than PIN-based passwords?

50 απαντήσεις